INTERNATIONAL STANDARD

ISO/IEC 27034-2

First edition
2015-08-15

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

Technologie de l'information — Sécurité des applications —

Partie 2: Cadre normatif de l'organisation

Reference number
ISO/IEC 27034-2:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27034 consists of the following parts, under the general title *Information technology — Security techniques — Application security*:

— *Part 1: Overview and concepts*

— *Part 2: Organization normative framework*

The following parts are under preparation:

— *Part 3: Application security management process*

— *Part 4: Application security validation*

— *Part 5: Protocols and application security control data structure*

— *Part 6: Security guidance for specific applications*

— *Part 7: Application security assurance prediction*

Introduction

General

Organizations must protect their information and technological infrastructures in order to stay in business. There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards improving application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The Organization Normative Framework (ONF) is the most important of those components.

The ONF is an organization-wide framework where all application security best practices recognized by the organization are stored. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself. It is the foundation of application security in the organization and all the organization's future application security decisions should be made by referring to this framework. The ONF is the authoritative source for all components and processes related to application security in the organization.

This part of ISO/IEC 27034 defines the processes required to manage the security of applications in the organization. These processes are presented in 5.4. It also introduces security-related elements of applications (processes, roles and components) that should be integrated into the ONF. These elements are presented in 5.5.

Finally, this part of ISO/IEC 27034 presents the Auditing the ONF process, needed by an organization for verifying its ONF and verifying compliance of all applications with the requirements and controls in the ONF. This process is presented in 5.4.8.

Purpose

The purpose of this part of ISO/IEC 27034 is to assist organizations to create, maintain and validate their own ONF in compliance with the requirements of this International Standard.

This part of ISO/IEC 27034 is designed to enable an organization to align or integrate its ONF with the organization's enterprise architecture and/or the organization's information security management system requirements. However, implementing an information security management system as described in ISO/IEC 27001 is not a requirement for the implementation of this International Standard.

Targeted Audiences

General

The following audiences will find value and benefits when carrying their designated organizational roles:

a) managers;

b) ONF committee;

c) domain experts;

d) auditors.

Managers

Managers should read this International Standard because they are responsible for the following:

a) improving application security through the ONF and other aspects of ISO/IEC 27034;

b) ensuring the ONF stays aligned with the organization's information security management system and application security needs;

c) leading the establishment of the ONF in the organization;

d) ensuring the ONF is available, communicated and used in application projects with proper tools and procedures all across the organization;

e) determining the appropriate level(s) of management that the ONF Committee reports to.

ONF Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee needs to

a) manage the cost of implementing and maintaining the ONF,

b) determine what components and processes should be implemented in the ONF,

c) make sure introduced components and processes respect the organization's priorities for security requirements,

d) review auditor reports for acceptance or rejection that the ONF conforms to this International Standard and meets the organization's requirements,

e) provide processes and tools for managing compliance with standards, laws and regulations according to the regulatory context of the organization,

f) communicate security awareness, training and oversight to all actors, and

g) promote compliance with the ONF for all application projects throughout the organization.

ONF development team

Experts who have been assigned by the ONF Committee with the task of developing and implementing one or more ONF element(s), who need to

a) develop and implement a designed ONF element,

b) determine training in the use of ONF elements by its different actors, and

c) collaborate in providing adequate training to actors.

Domain experts

Provisioning, operation, acquisition and audit experts who need to

a) participate in ONF implementation and maintenance,

b) validate that the ONF is useable and useful in the course of an application project, and

c) propose new components and processes.

Auditors

Auditors are personnel performing roles in the audit processes, who need to participate in ONF validation and verification.

NOTE Auditors may be external or internal to the organization, depending on the target and circumstances of the audit, and according to the organization's audit policies and conformance requirements.

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

1 Scope

This part of ISO/IEC 27034 provides a detailed description of the Organization Normative Framework and provides guidance to organizations for its implementation.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27034-1:2011, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

NOTE Additional detail about the relationship between ISO/IEC 27034 and other standards is available in ISO/IEC 27034-1:2011, 0.5.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27000, and ISO/IEC 27005 apply.

4 Abbreviated terms

ASLC	Application Security Life Cycle
ASLCRM	Application Security Life Cycle Reference Model
ANF	Application Normative Framework
ASC	Application Security Control
ASMP	Application Security Management Process
ONF	Organization Normative Framework

5 Organization Normative Framework

5.1 General

An organization's normative framework is the sum of all regulations, policies, practices, roles and tools used by the organization. Every organization should already have a normative framework, more or less formally documented.

The Organization Normative Framework (ONF) concept described in this International Standard is an organization-wide framework containing a subset of the organization's processes and components that are relevant to application security and are normative inside the organization.

Although an informal ONF is a first step towards securing the organization's applications, this International Standard recommends a formalized and standardized ONF, as described in this International Standard.

5.2 Purpose

The purpose of implementing the ONF is to:

a) assign responsibility for application security and establish a process that can evolve to improve application security visibility;

b) ensure all elements (components, roles and processes) involved in application security are approved by the appropriate decision-makers and accepted by all relevant actors and stakeholders;

c) minimize resistance to changes brought by these new application security elements;

d) standardize application security elements to ensure a uniform implementation and verification throughout the organization;

e) help the organization to improve its maturity level (as defined in ISO/IEC 15504 and other standards such as SEI/CMMI) by formalizing and revising all application security elements to keep them up to date with the organization's evolving environment; and

f) establish mechanisms to ensure that an appropriate level of security can be achieved in a cost-effective manner, for example, through reusing existing approved application security elements.

5.3 Principles

Organizations creating and maintaining the components and processes in the ONF should be guided by the following principles:

a) the contents of ONF should be adapted to the organization's business needs;

b) any element defined in the ONF should be approved by the ONF committee;

c) contents of the ONF should be available and communicated organization-wide;

d) because the threat context changes continuously and without notice, the organization should be prepared to review the ONF in response to those changes; and

e) the ONF should be auditable.

5.4 ONF Management Process

5.4.1 General

The organization should establish, implement, maintain and improve an organization-level process for the management of its ONF.

The ONF Management Process comprises six sub processes.

Four of them are adapted from the "Plan, Do, Check, Act" processes of the general PDCA model, and are tailored for the development and implementation of application security elements in the ONF.

The following table shows how ONF management sub processes map to the four stages of the PDCA model and to information security management system processes.

Table 1 — Mapping of PDCA stages, information security management system processes and application security-related ONF management sub processes

PDCA Stage	ISO/IEC 27001 **Information security management process**	ISO/IEC 27034 **ONF Management Process**
Plan	Planning	Designing the ONF
Do	Support / Operation	Implementing the ONF
Check	Performance evaluation	Monitoring and reviewing the ONF
Act	Improvement	Improving the ONF

Another sub process, "Establishing the ONF committee", is used first, to mandate the ONF committee and demonstrate appropriate accountable management's commitment to application security. Finally, the "Auditing the ONF" sub process is used for verifying the ONF and verifying compliance of applications with the requirements and controls in the ONF.

The organization should perform the ONF Management Process iteratively in order to incrementally implement the ONF. This reduces impact and achieves quicker gains by prioritizing in each iteration those elements that are more urgently needed.

A graphical representation of the ONF Management Process is shown in Figure 1. The figure also shows how this process relates to the organization's other management processes, and to the Application Security Management Process which makes use of the ONF for adding Application Security Controls to application projects.

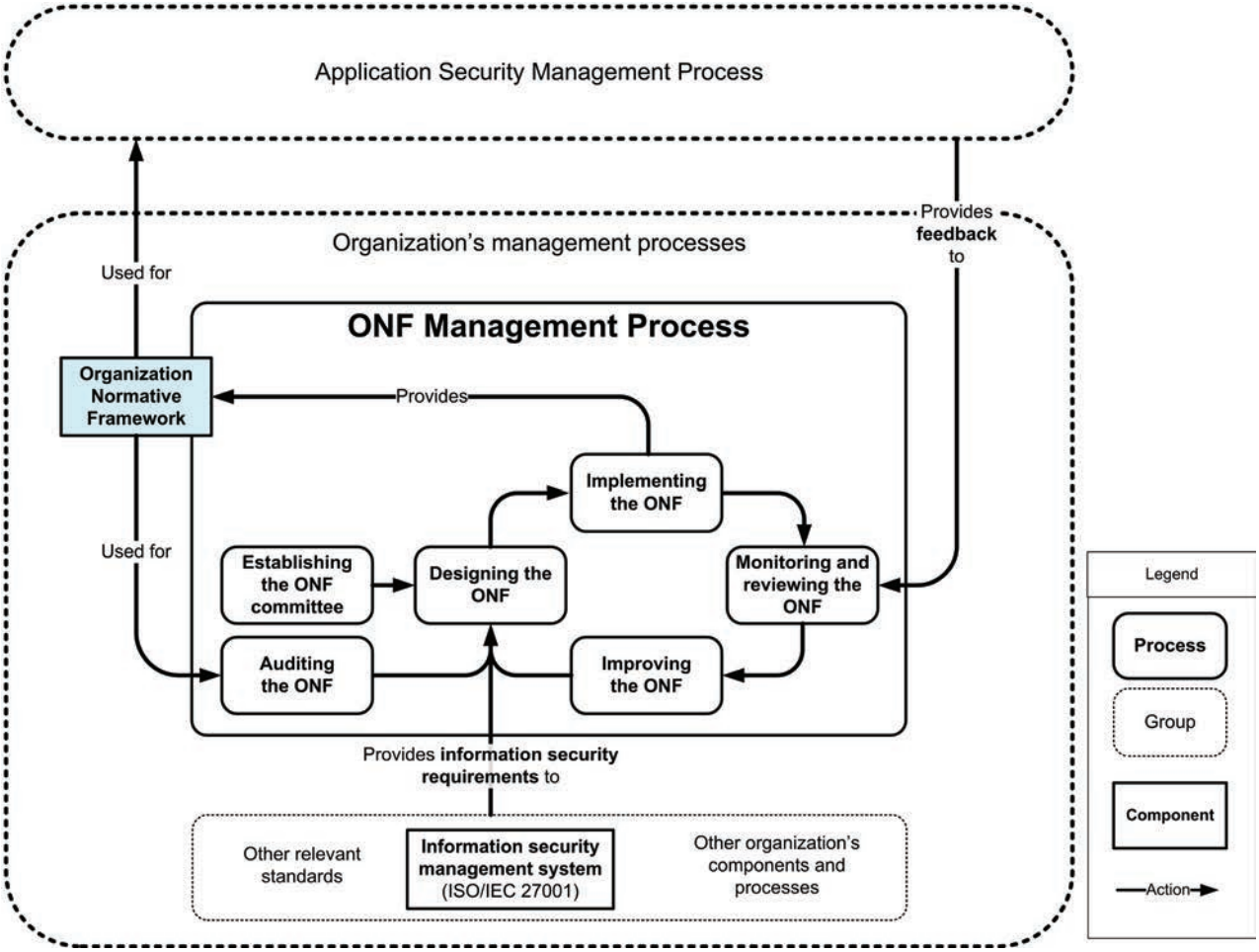

Figure 1 — ONF Management Process

5.4.2 Use of RACI charts in description of activities, roles and responsibilities

This International Standard uses RACI charts for assigning roles and responsibilities for carrying out activities in processes. Such charts identify actors responsible, accountable, consulted or informed for the realization of an activity. Abbreviations are used for describing responsibilities of actors. Those are enumerated in Table 2.

Table 2 — Abbreviations for responsibilities used in RACI charts

Code	*Responsibility*
R	*Responsible for the realization of an activity*
A	*Accountable for the realization of an activity*
C	*Consulted during the realization of an activity*
I	*Informed of the realization of an activity*

Use of RACI charts within organizations implementing this standard is not required. Organizations should align guidance provided in this standard with their own method of clarifying roles and responsibilities.

When conducting realization and verification activities, it is critical for organizations to determine the resources that are responsible, accountable, consulted, and informed. The tables below provide a starting point for discussion during the realization of an ONF.

5.4.3 Establishing the ONF committee

5.4.3.1 Purpose

The purpose of this process is to establish an ONF committee with the required authority and resources for the development, implementation and evolution of the ONF, and to demonstrate appropriate accountable management's commitment.

5.4.3.2 Outcomes

As a result of the successful performance of this process:

a) roles and responsibilities for ONF Committee members are defined;

b) a candidate is appointed for each role;

c) the ONF committee is officially mandated to establish and maintain the ONF and this is communicated within the organization;

d) the ONF committee is made accountable for the implementation, quality, and utilization of the ONF in the organization;

e) the ONF committee is provided with the necessary resources for assuming its responsibilities; and

f) the ONF committee is provided with sufficient authority for relevant internal communication.

5.4.3.3 Realization activities

Table 3 — RACI chart for realization of process "Establishing the ONF committee"

Realization activities	Managers
1) Define roles and responsibilities for ONF Committee members.	A/R
2) Appoint a candidate for each role.	A/R
3) Officially mandate the ONF committee to establish and maintain the ONF and communicate this within the organization.	A/R
4) Make the ONF committee accountable for the ONF implementation, quality, and utilization in the organization.	A/R
5) Provide the ONF committee with the necessary resources for assuming its responsibilities.	A/R
6) Provide the ONF committee with sufficient authority for relevant internal communication.	A/R

5.4.3.4 Verification activities

Table 4 — RACI chart for verification of process "Establishing the ONF committee"

Verification activities	Managers	Auditors
1) Verify the existence of official communication from appropriate accountable management demonstrating that outcomes a), b), c) and d), were achieved.	A	R
2) Evaluate from official communication from appropriate accountable management whether outcomes e) and f) were achieved.	A	R

5.4.4 Designing the ONF

5.4.4.1 Purpose

The purpose of this process is to determine goals for application security, determine which elements should be implemented in the ONF in the current iteration of the ONF management process, and design those elements.

5.4.4.2 Outcomes

As a result of the successful performance of this process:

a) the scope of the current iteration of the ONF management process is defined, approved by appropriate accountable management and communicated, and

b) in-scope ONF elements are designed.

5.4.4.3 Realization activities

Table 5 — RACI chart for process "Designing the ONF"

Realization activities	Managers	ONF Committee
1) Determine application security goals.	A	R
2) Define the scope and implementation strategy of the current iteration of the ONF management process.	A	R
3) Define the organization's application security posture, priorities and plans.		A/R
4) Establish an inventory and a security classification of information involved with applications and integrate it within the organization's information architecture.		A/R
5) Design ONF elements.		A/R

5.4.4.4 Verification activities

Table 6 — RACI chart for verification for process "Designing the ONF"

Verification activities	Managers	Auditors
1) Verify that the scope of the current iteration of the ONF management process is defined, approved by appropriate accountable management and communicated.	A	R
2) Verify that the ONF elements in scope for the current iteration are designed correctly.	A	R

5.4.4.5 Guidance

Possible inputs for this process are:

a) outcomes of the organization's security risk management process, such as organization-level security objectives or plans;

b) outcomes of the "Improving the ONF" process, such as documented needs to redesign ONF elements or design new ONF elements;

c) outcomes of the "Auditing the ONF" process;

d) outcomes of an organization's information security audit;

e) training needs, strategy, metrics, policies, and up to date knowledge of attacks and mitigations; and

f) other ISO/IEC standards including supply chain (27036), evaluation (15408), assurance (15026), software life cycle processes (12207), system life cycle processes (15288) – see ISO/IEC 27034-1:2011, 0.5 and Figure 1.

ONF elements that should be designed are described in 5.5. Specific guidance for the design of those elements is also found in 5.5.

ONF elements should be designed and built in an iterative process. In the course of this process, the ONF committee should:

a) prioritize elements based on the organization's priorities and available resources;

b) assign responsibility and sufficient resources for the design of in-scope elements;

c) monitor and validate the design of ONF elements;

d) integrate the ONF's processes into the organization's business processes;

e) ensure that the ONF's application security policy is aligned with the organization's other policies and the organization's information security management system;

f) ensure that the ONF is aligned with the organization's security architecture, information architecture and business architecture;

g) ensure that ONF risk management performance indicators are aligned with other performance indicators used in the organization;

h) ensure that ONF risk management objectives are aligned with the objectives and strategies of the organization;

i) ensure legal and regulatory compliance;

j) ensure that the outcomes of its activities are communicated to all relevant parties;

k) designate an information repository to act as the authoritative source for consolidating and communicating information on the ONF and all its elements;

l) establish communication and reporting mechanisms (internal, external, interfaces with application projects, etc.); and

m) provide guidance on how to implement the requirements from this International Standard in the organization, by establishing an application security management policy.

NOTE It should not be expected that every member or partner of the organization will read this International Standard. It should be expected that they conform to the policy.

When approving the scope of a given iteration of the ONF management process, appropriate accountable management should:

a) verify that the ONF and its management processes are compatible with the strategic direction, information security objectives and policy of the organization; and

b) verify that the ONF is aligned with and supports the organization's existing enterprise architecture.

When verifying that the ONF elements in scope for the current iteration are designed correctly, auditors may consider criteria such as:

a) definition of scope and implementation strategy of the current iteration of the ONF management process;

b) definition of the organization's strategic application security posture, priorities and plans;

c) establishment of an application security management policy;

d) inventory and security classification (i.e. in terms of confidentiality, integrity and availability) of information involved with applications integrated within the organization's information architecture;

e) definition of roles for the implementation project for every component and process in the ONF;

f) assignment of people to such roles;

g) results of projects monitoring; and

h) communication and reporting mechanisms.

5.4.5 Implementing the ONF

5.4.5.1 Purpose

The purpose of this process is to implement ONF elements that have been designed in the current iteration of the ONF management process, provide application security solutions such as components and processes, and distribute them to be used throughout the organization as application security guidelines, services or mandatory practices.

5.4.5.2 Outcomes

As a result of the successful performance of this process, ONF elements are developed and implemented, and training is provided to relevant actors for the use of implemented ONF elements.

5.4.5.3 Realization activities

Table 7 — RACI chart for realization of process "Implementing the ONF"

Realization activities	ONF Committee	ONF element development team	Domain experts
a) Analyse the impact and complexity of developing and implementing the ONF elements designed within the scope of the current ONF management process iteration.	A/R		C
b) For each designed ONF element: 1) assign a development team;	A/R		
2 communicate management objectives and direction to thedevelopment team;	A/R		
3) provide adequate resources to the development team;	A/R	C	
4) develop and implement the ONF element;	A	R	C
5) determine training to use the ONF element by its different actors; and		A/R	C
6) provide adequate training to actors.	A/R	C	C

5.4.5.4 Verification activities

Table 8 — RACI chart for verification of process "Implementing the ONF"

Verification activities	ONF Committee	Auditors	Domain experts
1) Verify that designed ONF elements are developed and implemented according to the outcomes of the "Designing the ONF" process.	A	R	C

Table 8 *(continued)*

Verification activities	ONF Committee	Auditors	Domain experts
2) Verify that training identified by the ONF element development team is provided to relevant actors.	A	R	C

5.4.5.5 Guidance

The following should be used as prerequisite inputs for this process:

a) ONF implementation strategy for the current iteration of the ONF management process; and

b) design of ONF elements for current iteration.

Where an organization chooses to outsource or acquire any ONF elements that affect conformity to the ONF requirements, it should be ensured that the ONF committee management requirements are communicated to and implemented by those entities to which elements have been outsourced or from which they are acquired.

When assigning a development team for the implementation of an ONF element, the ONF committee should make available to the team the required resources and expertise, notably in the form of domain experts for the particular domain for which the ONF element applies.

EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts.

When verifying that designed ONF elements are developed and implemented, auditors may consider criteria such as:

a) management of ONF projects and application security investments;

b) establishment of communication and reporting mechanisms of the ONF;

c) use of interfaces in application security projects for accessing the ONF elements;

d) communication of the importance of effective application security management, conforming to the organization's information security management system;

e) documentation and communication of information as defined in the ISO/IEC 27001:2013 International Standard;

f) implementation of ONF elements for all critical applications, depending on the ONF implementation strategy; and

g) accountability of everyone involved with the implementation and utilization of the ONF.

In addition, for each designed ONF element auditors may consider criteria such as:

a) identification of an owner;

b) management objectives and direction;

c) competence of persons doing work;

d) training to use the ONF element by its different actors; and

e) implementation and management of ONF element.

Specific guidance for the implementation of some ONF elements is found in 5.5.

5.4.6 Monitoring and reviewing the ONF

5.4.6.1 Purpose

The purpose of this process is to review ONF components and processes to ensure that they remain adequate for their purpose and are used in conformity with the organization's application security policy.

5.4.6.2 Outcomes

As a result of the successful performance of this process:

a) documented information is recorded as evidence of the results of reviews, and

b) needed improvements to ONF elements are identified and recorded.

5.4.6.3 Realization activities

Table 9 — RACI chart for realization of process "Monitoring and reviewing the ONF"

Realization activities	ONF Committee	Domain experts
1) Define standard methods for measurement, analysis and evaluation of ONF elements to ensure valid and repeatable results.	A/R	C
2) Monitor changes (see guidance).	A/R	
3) Review ONF elements, using defined standard methods for measurement, analysis and evaluation, to determine whether they are performing as expected.	A/R	C
4) Retain documented information as evidence of the results of reviews.	A/R	
5) Identify and record needed improvements to ONF elements.	A/R	C
6) Communicate needed improvements to application project teams as needed.	A/R	

5.4.6.4 Verification activities

Table 10 — RACI chart for verification of process "Monitoring and reviewing the ONF"

Verification activities	ONF Committee	Auditors
1) Verify the existence and quality of documented information recorded as evidence of the results of reviews.	A	R
2) Verify the existence and quality of recorded information about needed improvements to ONF elements.	A	R

5.4.6.5 Guidance

ONF monitoring and review should be performed at planned intervals or in reaction to a specific change in the organization's contexts, to ensure its continuing suitability, adequacy and effectiveness.

The following may be used as inputs for this process:

a) outcomes of the organization's information security risk assessment process;

b) changes in the ONF organization's contexts;

c) results of ONF audits;

d) feedback from interested parties;

e) status of preventive and corrective actions;

f) results from effectiveness measurements; and

g) records of application security incidents.

Feedback from application projects should also be used as an important input with regard to continuous improvement of quality and effectiveness of ASCs deployed in projects.

EXAMPLE 1 The value of the "cost" attribute of an ASC will typically be a rough estimate at first, and be better defined with feedback from projects.

EXAMPLE 2 With constant changes in a typical organization's technological context, some ASCs will no longer satisfy the security requirements of new application projects. They will eventually become obsolete and be removed from the organization's ASC library. This will help prevent the situation of an obsolete control becoming a vulnerability in itself.

ONF elements being monitored include artefacts from application projects. By monitoring those elements, the ONF committee ensures that all application projects correctly follow the ASMP, particularly that they:

a) correctly use the ONF components;

b) provide a Targeted Level of Trust and an Actual Level of Trust; and

c) perform a periodic application risk assessment.

When monitoring and reviewing an ONF element, the ONF committee should acquire the required resources and expertise, notably in the form of domain experts for the particular domain for which the ONF element applies.

EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts.

When verifying that the ONF monitoring and reviewing process was performed correctly, auditors may consider criteria such as:

a) definition and validation methods for monitoring, measurement, analysis and evaluation to ensure valid results;

b) inclusion of decisions related to continual improvement opportunities and the possible need for changes to the ONF;

c) documented information evidencing the results of reviews;

d) measurement and monitoring ONF elements; and

e) evaluation of whether actions have been effective.

5.4.7 Improving the ONF

5.4.7.1 Purpose

The purpose of this process is to:

a) improve the usability, suitability, adequacy and effectiveness of the ONF;

b) add missing elements required by changes in the organization's environment; and

c) keep the ONF aligned with the organization's information security management system.

5.4.7.2 Outcomes

As a result of the successful performance of this process:

a) ONF elements are improved,

b) needs to redesign ONF elements or design new ONF elements are documented, and

c) changes to ONF elements are recorded, properly documented and communicated.

5.4.7.3 Realization activities

Table 11 — RACI chart for realization of process "Improving the ONF"

Realization activities	ONF Committee	ONF element development team	Domain experts
1) Perform previously identified needed improvements to ONF elements.	A	R	C
2) Evaluate the need to redesign ONF elements or design new ONF elements.	A	R	C
3) Document such needs and communicate them to the "Designing the ONF" process.	A	R	C
4) Manage changes by performing organization processes such as change management, configuration management, etc.	A/R		
5) Ensure improvement information, such as purpose, objectives, security requirements addressed, description and verification criteria, is properly documented and communicated.	A/R		

5.4.7.4 Verification activities

Table 12 — RACI chart for verification of process "Improving the ONF"

Verification activities	ONF Committee	Auditors
1) Verify that previously identified needed improvements to ONF elements were performed.	A	R
2) Verify that any needs to redesign ONF elements or design new ONF elements are documented.	A	R
3) Verify that changes to ONF elements are recorded, properly documented and communicated.	A	R
4) Verify that changes were properly managed by performing organization processes such as change management, configuration management, etc.	A	R

5.4.7.5 Guidance

The organization may use the processes of the information security management system such as leadership, planning and performance evaluation, to achieve improvement.

Outcomes of the "Monitoring and reviewing the ONF" process may be used as input for this process, such as:

a) documented information recorded as evidence of the results of reviews, and

b) recorded information about needed improvements to ONF elements.

When improving an ONF element, the ONF committee should acquire the required resources and expertise, notably in the form of domain experts for the particular domain for which the ONF element applies.

EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts.

When verifying that the ONF improvement process was performed correctly, auditors may consider criteria such as:

a) evaluation of the need to plan actions to address risks and opportunities;

b) integration and implementation of these actions into the ONF, when applicable;

c) realization of opportunities for improvement;

d) change management; and

e) availability of improvement information, such as purpose, objectives, security requirements addressed, description and verification criteria.

5.4.8 Auditing the ONF

5.4.8.1 Purpose

The purpose of this process is to measure compliance of the ONF to the organization's application security requirements, particularly the organization's application security management policy. It is especially useful for some organizations that have to ensure that their ONF is compliant with the requirements of another ONF, e.g. a parent organization's or a regulatory organization's ONF.

EXAMPLE A government might implement an ONF with minimum requirements for all government agencies. An agency's ONF would then have to comply to the government's ONF, i.e. it would have to implement at least the requirements in the government's ONF. This compliance might be verified during an audit of the agency's ONF.

5.4.8.2 Outcomes

As a result of the successful performance of this process:

a) an ONF audit programme is implemented and managed,

b) ONF elements are audited according to the programme,

c) audit results are properly documented and communicated, and

d) audit results are used for continuous improvement of the ONF.

5.4.8.3 Realization activities

Table 13 — RACI chart for realization of process "Auditing the ONF"

Realization activities	Managers	Auditors	ONF Committee	Domain experts
1) Implement and manage an ONF audit programme for integrating ONF audit activities into existing auditing processes.	A	R	C	C
2) Ensure auditors received adequate training for auditing the ONF.	A/R			C
3) Audit the ONF.	A	R	C	C
4) Find root causes of non conformities and suggest solutions in the audit results.	I	A	C	R
5) Document and communicate audit results.	A	R	I	
6) Ensure audit results are provided as input to the "Monitoring and reviewing the ONF" process.		A/R	C	

5.4.8.4 Verification activities

Table 14 — RACI chart for verification of process "Auditing the ONF"

Verification activities	Managers	External auditor
1) Verify that ONF audit activities are performed according to the ONF audit programme.	A	R

5.4.8.5 Guidance

Appropriate accountable management should implement and manage an ONF audit programme, conduct the audits, and ensure competence of auditors, in addition to the guidance contained in ISO/IEC 27007.

In implementing an ONF audit programme, management should review the organization's existing audit processes, particularly the information security management system audit process if implemented, and devise a strategy to align or integrate the ONF audit process to such existing processes. Management should also consider guidelines for auditing management systems from ISO 19011:2011, 5.2.1.

The ONF committee should determine what specific ONF elements should be audited, and what specific activities need to be added to existing audit processes in order to meet the objectives set by management in the audit programme.

The ONF audit programme needs not only appropriate accountable management's approval but also the resources and independence to objectively demonstrate that the ONF satisfies such organization's application security requirements as:

a) responsibilities are clearly defined in RACI charts (or similar methods) and communicated;

b) ONF elements are cost-effective and updated;

c) change management processes are followed;

d) ONF management sub processes are completed;

e) verification activities of each ONF management sub process are performed; and

f) previous audit and risk assessment results are considered.

The following should be used as prerequisite inputs for this process:

a) previous audit and risk assessment results; and

b) requests provided by the information security management system.

When auditing the ONF, the ONF committee should acquire the required resources and expertise, notably in the form of domain experts for the particular domain for which audited ONF elements apply.

EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts.

External auditors mandated by appropriate accountable management should verify that the ONF audit process was performed considering:

a) establishment of the audit programme;

b) approval of audit programme and provision of resources;

c) reported results of ONF audit process;

d) list of root causes of non conformities and solutions;

e) evidence of monitoring solutions; and

f) improvement of the audit process.

NOTE These auditors may be external or internal to the organization, but should be external to the scope of application security in the organization and outside the sphere of authority of the ONF committee. As with any process, there should be a separation of duty constraint between the realization activities and the verification activities for this process.

5.5 ONF Elements

5.5.1 General

The ONF provides elements such as components and processes for addressing the application security needs of the organization. A simplified graphical representation of the contents of the ONF is shown in Figure 2.

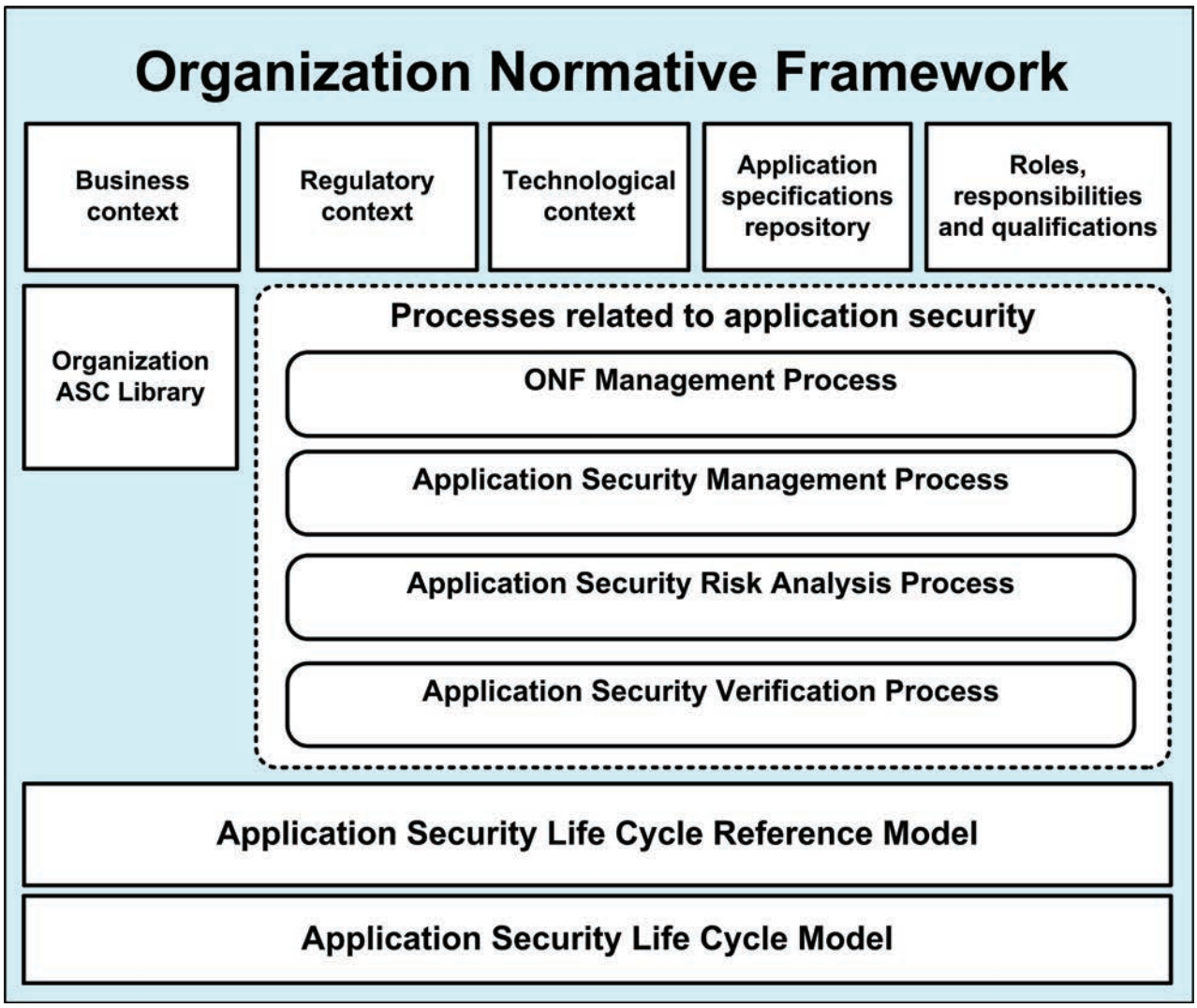

Figure 2 — Organization Normative Framework — simplified graphical representation

NOTE For the purpose of this document, two types of elements are defined: components and processes. Components are represented in Figure 2 using square boxes, and processes are represented using rounded boxes.

5.5.2 Business context component

5.5.2.1 Purpose

This component helps to identify security risks and requirements coming from the organization's business activities and provides values to be referenced in the "Requirements addressed" attribute of ASCs. It introduces an approved standard approach for mitigating risks associated with the organization's business domain.

5.5.2.2 Description

The business context is an inventory and documentation of all business processes, standards and best practices adopted by the organization that can have an impact on application projects. Such activities cause risks and the organization should determine security requirements for mitigating those risks. ASCs should be put in place for addressing those requirements. ASC builders need to indicate why an ASC is being provided, i.e. what security requirement the ASC is implementing. They will find the required information in the business context component of the ONF.

EXAMPLE 1 The organization's security policy is typically a direct source of security requirements. Some of them are relevant for application security. Non conformance to the security policy is a risk that an application owner usually does not tolerate. ASCs may be designed to satisfy specific requirements from the security policy.

EXAMPLE 2 A business process for building aircraft in the aeronautics business domain will bring a high level of risk and consequently numerous security requirements. As a result, numerous ASCs will usually be added to applications associated with this process.

5.5.2.3 Contents

The business context should provide:

a) a list of all business domains pertaining to all parts of the organization in which applications will run or will be used;

b) for each business domain, a list of processes, policies and best practices, that pertain to the usage of applications in that domain, such as:

   1) business, project management, development, risk analysis, operational, audit and control and change management processes;

   2) the organization's security policy;

   3) a list of the organization's information assets with their security classification;

   4) the development methodologies used by the organization;

   5) best practices for all programming languages employed by the organization and listed in the technological context; and

   6) standards, such as ISO/IEC International Standards and industry standards, to which the organization mandates compliance.

c) a list of risks brought by the above processes, policies and best practices, that are relevant to application security;

d) a list of security requirements for mitigating the above risks;

e) guidance and guidelines for ASC development, including:

   1) a list of ASC attributes that should or may be used for describing an ASC;

   2) a mapping to the attributes described in ISO/IEC 27034-5; and

3) as applicable, for each attribute, a set of allowed values, rules, nomenclature and dependencies.

5.5.2.4 Guidance

Information for building this ONF component should be obtained through an information security risk analysis. For organizations that have performed an information security risk analysis following the guidelines of ISO/IEC 27001:2013 and in conformance to the risk management process proposed in ISO/IEC 27005:2011, the effort required to build this component should be minimal.

The list of the organization's information assets with their security classification should be provided by the organization's information architecture. It is referred to as an "inventory of assets" in ISO/IEC 27001:2013, A.8.1.1.

The list of the organization's information assets should have sufficient granularity for efficient risk management. It is rarely the case that all information used by an application has the same security classification. It is more efficient to classify groups of information inside the asset.

EXAMPLE An information asset may be comprised of dozens of tables, only a few of which containing secret information.

The list of security requirements in this component should be specific enough that it will be directly useful for planning, designing and implementing ASCs.

An organization needs to add guidance and guidelines for ASC development because it may decide to implement the complete set of ASC attributes described in ISO/IEC 27034-5, or it may decide to implement a subset or subsets of it, or it may adapt it to its own needs or its existing documentation requirements for security controls.

Although the organization defines its own ASC guidance and guidelines, these should satisfy the minimum requirements enumerated in ISO/IEC 27034-5.

To ensure consistency, the ONF committee should make sure that ASC guidance and guidelines are created and available to ASC development teams in the early iterations of the ONF management process. The ONF management process will then allow for evolution of the ASC guidance and guidelines over time.

5.5.3 Regulatory context component

5.5.3.1 Purpose

This component helps to determine security risks coming from the organization's regulatory context; more specifically, the risks coming from the organization failing to comply with relevant laws and regulations. It provides values to be referenced in the "Requirements addressed" attribute of ASCs. It introduces an approved standard approach for mitigating risks associated with each relevant law or regulation.

5.5.3.2 Description

The regulatory context is an inventory and documentation of laws and regulations that can have an impact on application projects, in any of the organization's business locations, i.e. in countries or jurisdictions where the application is developed, deployed, or used.

This inventory will be especially useful for determining which laws and regulations are relevant to which application specifications associated with which business activities. Additional information should be added to the inventory for this purpose.

5.5.3.3 Contents

The regulatory context should provide:

a) a list of laws and regulations that are applicable according to the location where applications will be used for/by the organization;

b) a list of risks brought by the above laws and regulations, that are relevant to application security;

c) a list of security requirements for mitigating the above risks.

5.5.3.4 Guidance

Information for building this ONF component should be obtained through an information security risk analysis. For organizations that have performed an information security risk analysis following the guidelines of ISO/IEC 27001:2013 and in conformance to the risk management process proposed in ISO/IEC 27005:2011, the effort required to build this component should be minimal.

The list of security requirements in this component should be specific enough that it will be directly useful for planning, designing and implementing ASCs.

The organization should pay special attention (and may end up devoting considerable resources) to building a complete and adequate list of laws and regulations that are applicable according to the location where applications will be used for/by the organization. Laws and regulations will be applicable for each country where the application is designed, developed, acquired, provided, used and operated.

Architectural complexity, such as that present in distributed or cloud applications, may compound this problem. In a distributed architecture, components for user interface, for processing and for storage of data may physically reside in different countries and be subject to different laws.

Therefore the organization should,

a) resolve possible conflicts within the multiple laws and mandatory requirements, and

b) translate legal requirements into ASCs,

with the help of legal experts.

Describing a process for doing so is out of scope for this International Standard.

NOTE Such legal experts would then act as the domain experts in the "Implementing the ONF" and "Monitoring and improving the ONF" processes (see 5.4.5.3 and 5.4.6.3).

5.5.4 Technological context component

5.5.4.1 Purpose

This component helps to determine security risks coming from the organization's technological infrastructure. It provides values to be referenced in the "Requirements addressed" attribute of ASCs. It provides information as to what IT components may be used in support of ASCs that require such support.

5.5.4.2 Description

The technological context is a documentation of the organization's IT components (e.g. physical components, applications, services) and the organization's own best practices and rules which apply to the use of such components.

5.5.4.3 Contents

The technological context should provide:

a) a list of IT components used in the organization that are relevant to application security;

b) a list of risks brought to the organization by the above IT components; and

c) a list of security requirements for mitigating the above risks.

5.5.4.4 Guidance

Information for building this ONF component should be obtained from the organization's technological architecture, and through an information security risk analysis. For organizations that have performed an information security risk analysis following the guidelines of ISO/IEC 27001:2013 and in conformance to the risk management process proposed in ISO/IEC 27005:2011, the effort required to build this component should be minimal.

The list of security requirements in this component should be specific enough that it will be directly useful for planning, designing and implementing ASCs.

5.5.5 Application specifications repository

5.5.5.1 Purpose

This component helps to determine security risks coming from the organization's application specifications, and to mitigate the risk of incorrectly implementing and/or misusing these specifications. It provides values to be referenced in the "Requirements addressed" attribute of ASCs.

5.5.5.2 Description

The application specifications repository is a documentation of the organization's general IT functional requirements and corresponding pre-approved solutions. It should include all specifications, functionalities and services included in or offered by the organization's applications, including documents and best practices to implement, use and verify them.

Pre-approved solutions are often processes, products or code libraries that the organization makes recommended or mandatory practice through rules, policies or enterprise architecture within a specific environment. Such solutions are typically mature and continuously improved. The advantage of associating ASCs to such solutions which are in constant re-use is obvious.

5.5.5.3 Contents

The application specifications repository should provide:

a) a list of all application specifications included in or offered by the organization's applications;

b) for each specification, a list of processes and best practices approved by the organization, that pertain to its implementation, use, maintenance or verification;

c) a list of risks brought to the organization by the above application specifications; and

d) a list of security requirements for mitigating the above risks.

5.5.5.4 Guidance

Information for building this ONF component should be obtained from the documented architecture of the organization's applications and the organization's enterprise architecture.

Some information may be obtained through an information security risk analysis. For organizations that have performed an information security risk analysis following the guidelines of ISO/IEC 27001:2013 and in conformance to the risk management process proposed in ISO/IEC 27005:2011, the effort required to build this component should be minimal.

The list of security requirements in this component should be specific enough that it will be directly useful for planning, designing and implementing ASCs.

EXAMPLE An organization has an application called "M012 file tranfer service" and wants all future application projects to use this service for securely transferring documents between applications. The organization therefore needs to register this functionality in the application specifications repository, with relevant information such as the following:

a) the application specification is "transfer documents to entities external to the application and internal to the organization";

b) the list of processes and best practices includes "Whenever possible documents should always be transferred using the organization's M012 file transfer service", which is defined in an entry in the organization's Technological context in the ONF;

c) the list of risks includes "breach of confidentiality of documents being transferred between applications"; and

d) the list of security requirement includes "strong encryption of files between end points during transfer" and "server-and-client-side authentication".

In the course of its ONF management process, the organization should then build ASCs that correctly address the security requirements by mandating the use of the M012 file transfer service. Henceforth, for any application project requiring a document transfer functionality, this particular application specification would be selected, which would add these ASCs to the application project.

5.5.6 Roles, responsibilities and qualifications repository

5.5.6.1 Purpose

This component helps to determine security risks coming from the people involved with the organization's applications. It also helps to ensure that all critical roles for all processes are filled, that all responsibilities are defined, that conflicts of interest are avoided, and that people assigned to the roles have sufficient professional qualifications.

5.5.6.2 Description

The roles, responsibilities and qualifications repository is a documentation of roles, responsibilities and qualifications for actors involved with the organization's applications.

5.5.6.3 Contents

The roles, responsibilities and qualifications repository should provide:

a) a list of all roles involved with the organization's applications;

EXAMPLE Application Operator, Application Architects, security Architects, Technology Architects, Project Manager, Chief Security Officer, Application Owner, Developers, Directors, IT Infrastructure Team, Trainers, Supplier, Stakeholders, Security Manager, Laws and Regulations Specialists, Testers, Users;

b) a list of responsibilities assigned to the above roles; and

c) a list of required qualifications for performing the above responsibilities.

5.5.6.4 Guidance

Information for building this component may be provided by the organization's Human Resources department and the organization's business architecture.

The list of required qualifications in this component should be specific enough that it will be directly useful for planning, designing and implementing ASCs.

5.5.7 Organization ASC Library

5.5.7.1 Purpose

The ASC Library component is used by an organization for organizing ASCs according to the levels of trust they apply to, for communicating ASCs easily, and for selecting appropriate ASCs in the course of an application project.

5.5.7.2 Description

The ASC Library is the repository of ASCs available in the organization. Every ASC in this repository is associated with one or many level(s) of trust.

5.5.7.3 Contents

The ASC Library should provide:

a) a list of the levels of trust used in the organization, including information such as ID, name and description;

b) a list of ASCs assigned to each of the levels of trust; and

c) a hierarchical list of all ASCs maintained in the ONF.

5.5.7.4 Guidance

In the course of building its ASC library, the organization should consider as sources the following:

a) controls recommended by previous auditing activities;

b) controls associated with results of risk assessments;

c) controls included in widely accepted libraries such as ISO/IEC 27002, ISO/IEC 15408, and NIST SP 800-53.

d) controls developed and made available by third-parties such as providers, communities or other organizations.

Projects may apply additional system-specific approaches, subject to organizational rules. Where controls are derived from other sources, the originating source should be identified so that as the sources evolve the organization can keep up.

It is the ONF committee's responsibility to build an ASC library that satisfies the organization's particular security requirements and priorities.

Following this International Standard's application-centric view, the ONF committee may decide this goal is best achieved by analysing the organization's new or existing applications, determining their security risks and requirements, and implementing ASCs addressing these requirements according to priorities usually determined by risks.

As a prerequisite to this activity, the ONF committee should implement necessary ONF components in early iterations of the ONF management process.

EXAMPLE 1 In order to determine risks and priorities, a list of the organization's information assets with their security classification should be available in the business context component of the ONF (see 5.5.2.3).

All relevant ONF components (business context, regulatory context, technological context, roles, responsibilities, and qualifications repository, and application specifications repository) should be considered in the risk analysis to produce security requirements leading to development of ASCs.

Because ASCs link to security requirements, a change in security requirements may initiate a change in all related ASCs.

With such necessary input, as a result of the "Designing the ONF" process the ONF committee determines which applications should be analysed in the next iteration of the ONF management process. Some organizations may prioritize applications using information assets with a high security classification.

For each application, the ONF committee should select ASCs to be implemented in order to meet the application's security requirements. The ONF committee should then perform the "Implementing the ONF" process for these ASCs. See 5.5.8.3 for guidance on implementing ASCs.

The result is a set of ASCs, which the ONF committee should now include in the ASC Library, so that it can be used in application projects.

It can match the existing ASC library in three possible ways:

a) the entire set of ASCs already comprises an existing level of trust in the library, in which case nothing is added to the library – existing ASCs are simply updated;

b) an existing level of trust closely matches the full set of ASCs, in which case the library may be completed by ASCs from the set; or

c) a new level of trust is created in the library from the set of ASCs.

EXAMPLE 2 An organization performs this process for the first time. The ASC Library is empty. The ONF committee decides to include the new set of ASCs as a new level of trust in the ASC Library. It labels this level of trust "C2 client-server application with no exposure to the internet", where "C2" is the confidentiality classification for the application's information assets, on a scale ranging from C1 to C4 (C4 being the highest confidentiality impact and C1 being the lowest). This level of trust will be used for any similar application using C1 or C2 information assets.

EXAMPLE 3 The same organization performs this process again for another existing application which is quite similar to the one in example 2, except that it uses some C3 assets and has a few more security controls. Since the new set of ASCs closely matches the existing level of trust, the ONF committee decides to update the existing level of trust and re-label it "C3 client-server application with no exposure to the internet". This level of trust will be used for any similar application using C1, C2 or C3 information assets. The rationale for this decision is that the extra cost of using "too many" security controls for C1 and C2 applications will be more than compensated by the huge gain in efficiency of reusing an existing level of trust.

EXAMPLE 4 The same organization performs this process for a new project for an application using C2 information and offered as an internet service. The set of ASCs implemented for this application is significantly different (50 % new ASCs) from the ones existing in the ASC Library. The ONF committee decides to insert it as an entirely new level of trust in the Library, and labels it "C2 web application exposed to the internet". Because 50 % of its ASCs are re-used, the organization still benefits from a gain in efficiency.

EXAMPLE 5 The same organization performs this process for a new application which is similar to the one in Example 2, except that it uses mainly C4 assets, which are considered critical for this organization and are subject to particularly stringent legal requirements and scrutiny. The set of ASCs implemented for this application is significantly different from any existing level of trust in the ASC Library: it comprises 70 % new ASCs, most of which are monitoring and accountability controls in the utilization stage of the application's life cycle, which are quite costly to implement. The ONF committee decides to insert it as an entirely new level of trust in the ASC Library, and labels it "C4 client-server application with no exposure to the internet". This level of trust will be used for any similar application using C4 information assets, but only for these because of the huge cost of operating an application at this level of security. Because 30 % of its ASCs are re-used, the organization still benefits from a gain in efficiency.

EXAMPLE 6 An organization has developed internally a critical application known as "The Keep", which has been made as secure as the organization could achieve. In the course of a new critical application project, the application owner declares he wants to trust this new application as much as he trusts The Keep. The ONF committee decides to perform the above process in priority for The Keep. The resulting level of trust is labelled "Same as The Keep". The ONF committee then performs the above process for the new application, and determines that its security requirements are indeed more than adequately covered by the ASCs in the "Same as The Keep" level of trust. The development team uses the ASCs in this level of trust for the new application, and the application owner is satisfied that his level of trust is "Same as The Keep". In addition, the cost of security controls for the new application is reduced because a large part of it has already been taken up by The Keep's project.

As shown in the previous examples, and as stated in ISO/IEC 27034-1, a level of trust is simply a label given to a set of ASCs responding to the security requirements of one or many applications, and thus the level at which the organization can trust the application, hence the name. There is no prescribed nomenclature for this label, and there is no requirement for any kind of ordering among levels of trust.

NOTE 1 ISO/IEC 27034-1:2011, Figure 5 depicts levels of trust labelled 0 to 5, however this is only an example.

When integrating controls from a third-party, the organization should map the third-party's specific information to its own.

EXAMPLE 7 Following a recommendation from an ASC development team, an organization decides to purchase ASCs from a third-party ASC vendor, in order to implement different types of security testing for its own applications. Naturally, the purchased ASCs are designed for a different ASC Library and their recommended levels of trust do not match the organization's. Fortunately, the purchased ASCs were exported in the open and portable exchange language for ASCs recommended in ISO/IEC 27034-5, which includes the vendor's range of levels of trust in the definition of the ASCs. The organization compares this range to its own and establishes a simple mapping which allows it to integrate the ASCs into its own ASC Library.

NOTE 2 ISO/IEC 27034-6 provides a more detailed case study for the integration of third-party ASCs.

EXAMPLE 8 Annex B provides a summary description of an actual project for implementing the ONF in a large organization. The workflow used for this project is specific to the organization and was designed by the project team. It is shown as an example, and not as a required process for implementing the ONF in any other organization.

5.5.8 Application Security Control

5.5.8.1 Purpose

This component documents a security control in order to facilitate its approval, maintenance, usage, verification and communication.

5.5.8.2 Contents

ISO/IEC 27034-1:2011 provides an overview of the Application Security Control (ASC) component and a description of the data that comprises an ASC. Organizations can implement ASCs using a narrative or custom approach that includes minimum recommendations identified in ISO/IEC 27034-1:2011, 8.1.2.6.5.

5.5.8.3 Guidance

Application Security Controls are contained in the Application Security Controls Library.

An ASC should be created to formally describe each security activity that the organization wants performed at any stage of the life cycle of any of its applications.

Other ONF components described in this International Standard provide sets of allowed values for the following attributes mentioned in ISO/IEC 27034-1:2011, 8.1.2.6.5.3 and 8.1.2.6.5.4 and ISO/IEC 27034-5, 5.2:

a) requirements addressed (see 5.5.2.3, 5.5.3.3, 5.5.4.3 and 5.5.5.3);

b) roles, responsibilities and qualifications required (see 5.5.6.3); and

c) "When" (see 5.5.9.3).

ISO/IEC 27034-5 and ISO/IEC 27034-5-1 provide a more detailed structure and types for all the ASC data elements. Organizations may use this for building interoperable ASCs that can be communicated to other organizations.

In addition, this structure provides data fields that help the organization to cross-reference its ASC information and make it available to organization processes such as change management, compliance management and risk management.

ISO/IEC 27034-6 provides examples of ASCs built using this data structure.

The roles involved in security activities and verification measurements of ASCs should be clearly defined and documented along with other roles in the organization's application life cycle. They should be assigned clear responsibilities, for example by using RACI charts.

Evidence should be provided to ensure that roles involved in security activities and verification measurements have the required qualifications.

As with any ONF element, an organization should create, review and improve ASCs by way of the ONF management processes described in 5.4.4, 5.4.5, 5.4.6 and 5.4.7.

As a result of the "Designing the ONF" process, the ONF committee should select ASCs to be developed (i.e. created or maintained) during the current ONF management cycle, according to current organization's priorities. For ASCs, such priorities are often dictated by the organization's current risks and application projects' immediate needs.

The ONF committee should then perform the "Implementing the ONF" process. For each of the selected ASCs, or group of related ASCs, it should:

a) assign an ASC development team, the composition of which depends on the body of knowledge required in order to come up with an adequate solution (i.e. "security activity" and "verification activity") for a particular ASC's "security requirements" at the "recommended Levels of trust";

   NOTE When creating, reviewing or improving an ASC, the ONF committee should acquire the required resources and expertise, notably in the form of domain experts for the particular domain to which the ASC applies;

   EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts;

b) communicate management objectives and direction to the development team, which is mainly done through the security requirements and the recommended Levels of trust for the ASC;

c) provide adequate resources to the development team, in the form of time, budget, project management, tools, documentation, training and technical resources such as development laboratories;

d) allow the development team to design, develop and implement the ASC, which usually should be done through project activities;

e) validate the design, approve the newly developed ASC and include it in the ASC Library;

f) provide adequate training to actors, as determined by the development team, according to the roles, responsibilities and qualifications required for both the security activity and the verification activity of the ASC.

In the course of developing and implementing the ASC, the development team should provide an adequate solution to the security requirements and recommended Levels of trust communicated by the ONF committee. The team should:

a) acquire a complete understanding of the security requirement communicated by the ONF committee, its history and context. This often involves meeting with the organization's bodies and persons at the origin of the requirement, such as an application project team, or reading

documented requirements from an application project. It is essential to understand the meaning of the recommended Level(s) of trust for the ASC. This information comes from the ASC Library.

b) build an inventory of existing solutions. This may involve searching the ASC Library for existing ASCs addressing the same or similar security requirements, searching for existing ASCs outside of the organization, or searching for existing controls that have not yet been described in an ASC data structure.

c) acquire sufficient understanding of the organization's existing legal, business and technological contexts as applies to the security requirement, in order to eliminate solutions that would not conform or integrate easily with the organization's contexts.

d) examine different solutions and select the one that best minimizes the security risk identified in the security requirement, in the organization's contexts.

e) acquire a complete understanding of the organization's guidance and guidelines for the ASC it is developing. This information should be provided by ONF components. For example:

EXAMPLE 1 ASC guidance and guidelines provide the ASC attributes, domains of values, rules, nomenclature and dependencies for each attribute;

EXAMPLE 2 The business, regulatory and technological contexts provide requirements to be referenced in the "Requirements addressed" attribute of the ASC;

EXAMPLE 3 The roles, responsibilities and qualifications repository provides values for roles and responsibilities in the description of security and verification activities of the ASC;

EXAMPLE 4 The Application Security Life Cycle Reference Model provides values for the "when" attribute in the description of security and verification activities of the ASC;

f) document the solution in the form of an ASC by providing values to each ASC according to the organization's guidance and guidelines.

The new ASC may be one of the following:

a) an entirely new ASC; or

b) a rework of an existing ASC, in which case the new ASC may be:

1) a new instance of an existing ASC for a different requirement,

2) a more precise instantiation of a parent ASC; or

3) a new version of an existing ASC, with augmented or corrected content.

The new ASC should be positioned adequately in the ASC Library in order to facilitate its reuse, i.e. it should be linked, via its "parents" attribute, to adequate parent ASCs. Additionally, the new ASC may be inserted in the library as a parent to other ASCs, which should then be modified to reflect this parenting.

NOTE As the ASC Library becomes more and more complex, the organization should consider the use of a technological solution for its management.

In many cases, and especially when the organization is in the early stages of implementing the ONF, the development team's work will consist mostly of transcribing existing controls in the ASC data structure. This structure allows for links to be added to an existing control's documented design, or even for such documents to be attached to the ASC.

As more organizations transcribe controls in ASC templates and make them available, it will become easier for development teams to acquire ASCs from other organizations, and adapt them for the organization's requirements and contexts. In such cases it is recommended to make such adapted ASCs new versions of the acquired ASCs, keeping the original versions for reference purposes.

Each ASC should be complete, i.e. the development team should provide a value for each attribute in the template, even if the value is incomplete or yet unknown. This provides more information than an

empty attribute, because it indicates that the attribute was actually considered and a decision has been made about its value, even if the decision was that the value is not yet known.

5.5.9 Application Security Life Cycle Reference Model

5.5.9.1 Purpose

The purpose of this component is to:

a) help an organization demonstrate when ASCs are applied in an application's life cycle (i.e. provide a set of allowed values for the "When" attribute of ASCs);

b) provide a reference for roles implicated in performing an ASC's activities or tasks;

c) help the organization to validate each of its application life cycles by specifying all activities and actors potentially involved in application security;

d) help the organization to ensure that security concerns are correctly addressed at all stages of its application life cycles;

e) help the organization to minimize the cost and impact of introducing ISO/IEC 27034 practices in its application projects by retaining its existing application life cycles;

f) facilitate communication between teams involved in different domains of knowledge;

g) provide the organization with a standard model for aligning ASCs between its application project teams, despite differing application life cycles; and

h) provide organizations with a standard model for sharing ASCs with other organizations, despite differing application life cycles.

5.5.9.2 Description

This component provides a reference application security life cycle model that maps to an organization's own model(s). It provides a standardized list of activity areas, activities and roles involved in management, software engineering, IT infrastructure and application audit, as a reference model for an application security life cycle, to help an organization to uniformly identify and communicate when in the application life cycle and by whom ASCs should be implemented.

As illustrated in Figure 3, this reference model is divided horizontally into two main stages: Provisioning, during which activities are performed for obtaining and deploying an application, and Operation, during which post-deployment activities are performed.

Provisioning and Operation stages can be further divided into stages as follows:

a) Provisioning stages consist of three stages: Preparation, Realization and Transition;

b) Operation stages consist of three stages: Utilization and maintenance, Archival and Destruction.

This reference model is divided vertically into four main layers:

a) Application management: this layer comprises activities from the governance domain, such as project management and application operation management. Such activities are usually performed within processes defined in the organization's information security management system;

b) Application provisioning and operation: this layer comprises activities relating to the provisioning and use of the application itself. Such activities are usually performed within processes recommended by standards such as ISO/IEC 15026 (all parts), ISO/IEC 15288, ISO/IEC 12207 and ISO/IEC 21827;

c) Infrastructure management: this layer comprises activities relating to the organization's IT service management infrastructure supporting the application. Such activities are usually performed within processes recommended by standards such as ISO/IEC/TR 20000-4; and guidance products, such as ITIL; and

d) Application audit: this layer comprises activities relating to control and verification. Such activities are usually performed within processes recommended by standards such as ISO/IEC 15288, ISO/IEC 12207 and industry practice documents, such as COBIT.

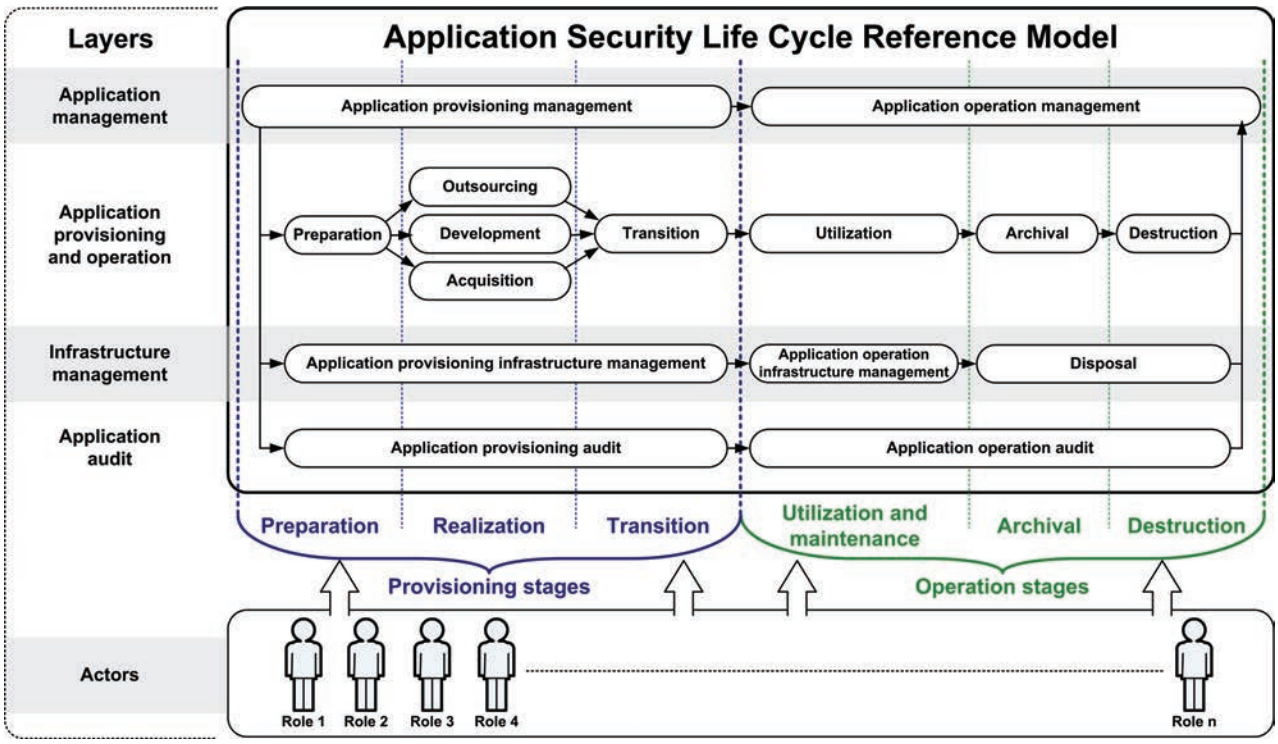

Figure 3 — Graphical representation of the Application Security Life Cycle Reference Model

5.5.9.3 Contents

5.5.9.3.1 Roles

The Application Security Life Cycle Reference Model should provide a list of roles for all actors involved in Application Security Life Cycle Reference Model activities, to help the organization to uniformly identify and communicate roles, responsibilities and required qualifications, by providing a set of allowed values for the "Roles", "Responsibility" and "Qualifications required" attributes of ASCs.

For this set of allowed values, it is highly recommended that the organization use the standardized list of roles provided in ISO/IEC 27034-5. This allows sharing of ASCs with different project teams within the organization, or with different organizations.

5.5.9.3.2 Activities

The Application Security Life Cycle Reference Model should provide a detailed list of activities as a set of allowed values for the "When" attribute of ASCs. The organization should use the standardized list of activities provided in ISO/IEC 27034-5-1. This allows sharing of ASCs with different project teams within the organization, or with different organizations.

Activities usually performed in the stages of the Application Security Life Cycle Reference Model and shown in Figure 3 are described as follows.

5.5.9.3.2.1 Application provisioning management

Application provisioning management activities are carried out by project managers and organizational managers, during the provisioning stages of the application life cycle.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from the Project processes group defined by ISO/IEC 12207, such as Human Resource management Process, Project Planning Process, Project Assessment and Control Process, and Decision Management Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as initiating, planning, execution, monitoring and control, and closing.

5.5.9.3.2.2 Application operation management

Application operation management activities are related to the management and use of the application during the operation stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Decision Management Process and Information Management Process.

Usually, an application is under the responsibility of its owner who may elect to share some of this responsibility with other actors such as user managers.

Changes to the application during operation stages, such as changes stemming from new regulatory requirements or threats, should be initiated by the application owner, who is responsible for ensuring that the application correctly and continuously addresses the organization's changing security needs.

Through these processes, the application owner will provide the organization's information security management system with the needed assurance and evidence that the governance of application projects is being addressed.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as initiating, planning, execution, monitoring and control, and closing.

5.5.9.3.2.3 Preparation

During the preparation stage, the provisioning team carries out preliminary or preparation activities. Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as 6.3.3 Decision Management Process and 6.3.6 Information Management Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as initiation and planning.

5.5.9.3.2.4 Outsourcing

During the realization stage, activities related to the implementation of software are performed by the provisioning team. If the organization is outsourcing some implementation activities, it might need to add specific ASCs to its implementation activities in order to achieve the application's Targeted Level of Trust. For this reason, the Application Security Life Cycle Reference Model presents a specific activitiy area for outsourcing.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Acquisition Process, Software Documentation Management Process, Software Configuration Management Process and Risk Management Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as realization and transition.

5.5.9.3.2.5 Development

Activities related to the implementation of software are performed by the provisioning team during the realization stage. If the organization is performing internally some implementation activities, the ASCs added to its implementation activities might be different from those added when purchasing or outsourcing the implementation or application components. For this reason, the Application Security Life Cycle Reference Model presents a specific area for development activities resulting in the implementation of internally developed software.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Risk Management Process, System Architectural Design Process, Software Architectural Design Process, Software Detailed Design Process, Software Construction Process, Software Documentation Management Process, Software Configuration Management Process, Software Verification Process, Software Validation Process, Software Review Process, Domain Engineering Process and Reuse Asset Management Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as inception, elaboration, construction and implementation.

5.5.9.3.2.6 Acquisition

Acquisition activities may be carried out by the provisioning team for the purpose of obtaining externally or purchasing the product and/or service that satisfies the needs of the organization. Specific ASCs may be added to those activities. For this reason, the Application Security Life Cycle Reference Model presents a specific area for acquisition activities resulting in the implementation of acquired application components.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Acquisition Process, Software Documentation Management Process, Software Configuration Management Process, Risk Management Process and Implementation Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan and close.

5.5.9.3.2.7 Transition

This area in the Transition stage includes activities performed by the provisioning team for preparing, configuring, testing and deploying the application in the operating environment defined by the organization

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Configuration Management Process, System Integration Process and System Qualification Testing Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as planning, development and testing.

5.5.9.3.2.8 Utilization

Activities performed during the Utilization and maintenance stage are involved in the actual use of the application in the operating environment by all users including end-users. Such activities include user and access management, logging, monitoring, security training, etc.

Other activities are carried out for software maintenance and change management, including the updating of application software in order to meet changing information requirements, such as adding new functions and changing data formats. It also includes fixing bugs and adapting the software to new hardware devices.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Operation Process and Software Maintenance Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as utilization and maintenance,

5.5.9.3.2.9 Archival

Archival activities are performed by the operation team when the application is no longer needed in its active state. They include the archival of all the application's information, including the archival of all tools and processes to protect and securely access this information even if the application is not running in the operating environment anymore.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as the Software Disposal Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan, perform and verify.

5.5.9.3.2.10 Destruction

Destruction activities are involved in the secure destruction of all the application's information, including user data, organization's information, user logs, application parameters, etc.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as the Software Disposal Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan, perform and verify.

5.5.9.3.2.11 Application provisioning infrastructure management

Application provisioning infrastructure management activities are involved in providing and maintaining a secure technological infrastructure in support to the activities of the provisioning team. This includes services, facilities, tools, and communications and information technology assets in the development environment and various test environments.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Infrastructure Management Process and Configuration Management Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as installation, operation, maintenance, support and archival.

5.5.9.3.2.12 Application operation infrastructure management

Application operation infrastructure management activities are involved in providing and maintaining a secure technological infrastructure for the operation stages of an application's life cycle. This includes services, facilities, tools, and communications and information technology assets in the application's operating environment.

Other activities should also be carried out during the operation stages for the secure maintenance of the infrastructure supporting the application. Infrastructure maintenance includes system and network hardware maintenance, backup and recovery, disaster recovery, etc.

Such activities are usually performed as part of organization-wide processes. These include system engineering processes from ISO/IEC 15288 such as Operation Process and Maintenance Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as support, operation, maintenance and archival.

5.5.9.3.2.13 Disposal

Disposal activities are carried out in order to provide an assurance that all information stored on the servers, systems and others technological components used by an application are securely deleted. This allows for the disposal or recycling of these components without undue security risk for the organization.

Such activities are usually performed as part of organization-wide processes. These include system engineering processes from ISO/IEC 15288 such as the Disposal Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan, perform and verify.

5.5.9.3.2.14 Application provisioning audit

Audit activities may be performed on all activities, actors, processes, artefacts and application components used or produced during the application's life cycle.

These activities may be performed once or periodically by internal or external audit teams, depending on the Targeted Level of Trust of the application project. They provide the application owner with the needed assurance and evidence that security requirements for the application are met as expected.

Audit activities performed during the provisioning stages are usually different from those carried out during the operation stages. Organizations developing but not operating applications (such as software vendors) might never need to audit applications in operation stages. For this reason, the Application Security Life Cycle Reference Model presents a specific area for audit activities performed during provisioning stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Audit Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan, acquire, implement, deliver, support, monitor and evaluate.

5.5.9.3.2.15 Application operation audit

Audit activities performed during the operation stages are usually different from those carried out during the provisioning stages. Organizations operating only acquired applications might never need to audit applications in provisioning stages. For this reason, the Application Security Life Cycle Reference Model presents a specific area for audit activities performed during operation stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Audit Process.

For a more precise specification of when security activities should be performed, the organization may further subdivide this activity area into sub areas such as plan, acquire, implement, deliver, support, monitor and evaluate.

5.5.10 Application Security Life Cycle Model

5.5.10.1 Purpose

The purpose of this ONF component is to:

a) help the organization to discover and formally describe the application security life cycle model(s) that it is already using;

b) help the organization to complete these models if needed with the help of the Application Security Life Cycle Reference Model described in this International Standard (i.e. add layers, stages, activities or actors);

c) facilitate communication of ASCs to application development teams; and

d) facilitate integration of ASCs with other activities already performed by application development teams.

5.5.10.2 Description

An application security life cycle model is based on an application life cycle model but is used for managing application security activities. It should present layers, stages and activities.

5.5.10.3 Contents

This ONF component should provide a mapping of one or more life cycles already in use in the organization with the Application Security Life Cycle Reference Model.

5.5.10.4 Guidance

Different organizations use different life cycle models. It is also usual practice in organizations that different life cycle models are used by different development teams, in different parts of the organization, in different projects. This International Standard does not propose to impose a standardized life cycle to organizations or application development teams.

For this reason, ASCs, which in the ONF make references to activities from the standardized Application Security Life Cycle Reference Model (see 5.5.9), should be "translated" before being communicated to application teams, so that they can be integrated with each team's familiar life cycle model and activities.

The mapping provided by this component is used for this purpose. It may be as simple as the "Enumeration types" tables provided in ISO/IEC 27034-5-1, with a column added for each of the organization's life cycle models. ISO/IEC 27034-6 illustrates this method with a case study about "using the ASLCRM to facilitate implementation of ASCs by different development groups inside an organization".

Provisioning stages in the organization's application security life cycle model(s) should include all of the organization's application provisioning activities. Operation stages in the organization's application security life cycle model(s) should include all of the organization's application operation activities.

It is possible that layers, stages, activities or actors need to be added to an application security life cycle model, in order to ensure that each ASC required by an application's Targeted Level of Trust can be adequately applied during the application's life cycle.

The need for developing secure applications may require continuous improvement of the organization's application life cycle models, supported by the ONF management process and based on previous audit findings and risk assessment results, in order to guarantee that developed applications offer better resistance to attacks and do not present unacceptable security risks.

While reviewing and improving its Application Security Life Cycle Model, the ONF committee and the collaborating domain experts should be aware of the importance of defining, implementing,

maintaining and communicating an Application Security Life Cycle Model in accordance with its business and security objectives by organizing normative elements, application security controls, and activities throughout an application life cycle.

While reviewing and improving the Application Security Life Cycle Model, the following should be considered as inputs:

a) the Application Security Life Cycle Reference Model proposed by this International Standard (see 5.5.9);

b) the organization's application life cycle(s) and life cycle processes;

c) the organization's software development methodology;

d) the organization's Application Security Controls;

e) application security risk assessment results; and

f) feedback from the organization's developers, software engineers, and users, among other stakeholders.

5.5.11 Application Security Management Process

5.5.11.1 Purpose

The Application Security Management Process allows an organization to manage security for each application used by an organization.

5.5.11.2 Description

The Application Security Management Process is the overall process for managing security for each application used by an organization. It is a specialization of the risk management process presented in ISO/IEC 27005.

5.5.11.3 Outcomes

As a result of performing this process in the course of an application project:

a) the application's requirements and environment are determined;

b) the application's information security risks are assessed;

c) the application's security requirements are determined from the risk assessment, and expressed as the application's Targeted Level of Trust;

d) risk treatment is initiated by selecting appropriate ASCs according to the application's Targeted Level of Trust ;

e) the application's information security risks are treated by performing security activities and verification measurements defined in the selected ASCs; and

f) the application's residual risk is measured by determining the application's Actual Level of Trust by way of the Application Security Verification Process (5.5.13).

5.5.11.4 Realization activities

Table 15 — RACI chart for realization of the Application Security Management Process

Realization activities	Application owner	Application development team	Auditor
1) Perform step "Specifying the application requirements and environment".	A	R	
2) Perform step "Assessing application security risks".	A	R	
3) Perform step "Creating and maintaining the Application Normative Framework".		A/R	
4 Perform step "Provisioning and operating the application".		A/R	C
5) Perform step "Auditing the security of the application".	A	C	R

5.5.11.5 Verification activities

Table 16 — RACI chart for verification of the Application Security Management Process

Verification activities	ONF committee	Application owner	Application development team	Auditor
1) Verify that step "Specifying the application requirements and environment" is performed correctly in the course of the organization's application project.	A	C	C	R
2) Verify that step "Assessing application security risks " is performed correctly in the course of the organization's application project.	A	C	C	R
3) Verify that step "Creating and maintaining the Application Normative Framework" is performed correctly in the course of the organization's application project.	A		C	R
4) Verify that step "Provisioning and operating the application" was performed correctly in the course of the organization's application project.	A		C	R
5) Verify that step "Auditing the security of the application" was performed correctly in the course of the organization's application project.		A	C	R

5.5.11.6 Guidance

An overview of the 5 steps mentioned in 5.5.11.4 is presented in ISO/IEC 27034-1:2011, Clauses 7 and 8. A detailed description of the Application Security Management Process is the subject of ISO/IEC 27034-3 and further guidance will be provided in that International Standard.

The auditor responsible for conducting verification activity 5 in Table 16 should be independent of the auditor that carries out activity 5 in Table 15. Independence of auditor towards auditee should be demonstrated.

5.5.12 Application Security Risk Analysis Process

5.5.12.1 Purpose

Identify and evaluate application security risks in the whole application life cycle, to provide an accurate and repeatable application security risk analysis process and risk analysis tools approved by the organization.

5.5.12.2 Description

The Application Security Risk Analysis Process is the process for understanding the risk exposures for each application used by an organization. It is a specialization of a part of the risk management process presented in ISO/IEC 27005.

5.5.12.3 Contents

This component of the ONF is a documentation of processes, activities and tools approved by the organization for the purpose of conducting an information security risk analysis for which the scope is an application.

This ONF component should identify the security exposure of an application based on vulnerabilities, threats and business impacts associated with the assets (components) of the application, and provide prioritization of the risks arising.

5.5.12.4 Guidance

The organization should select or define an application security risk analysis process that is adequate for analysing application security risks. This is not necessarily the case for all risk analysis processes – most of them were designed for organizational risk and may not scale down easily.

This process should be able to guide the identification of application security exposure based on an established scope and considering assets (components) associated to the application. It should focus on knowledge about the operation environment where the application is used to identify which application components are vulnerable to specific threats and the consequences that losses of confidentiality, integrity and availability may have for the components.

The application security risk analysis process should be used while performing Step 2 “Assessing application security risks” of the ASMP, which is described in ISO/IEC 27034-1:2011, 8.3.3. Therefore, it should use as input the knowable information output from Step 1 “Specifying the application requirements and environment” of the ASMP, such as:

a) the application’s business, technological and regulatory contexts; and

b) the application’s specifications.

The output of the application security risk analysis process should be:

a) a list of security risks for the application; and

b) a list of security requirements for the application for reducing the security risks.

This has to be suitable as to help the project team to select appropriate ASCs for addressing the security requirements, i.e. to select the application’s Targeted Level of Trust.

Figure 4 shows how the application security risk analysis is an essential step in determining the application’s Targeted Level of Trust.

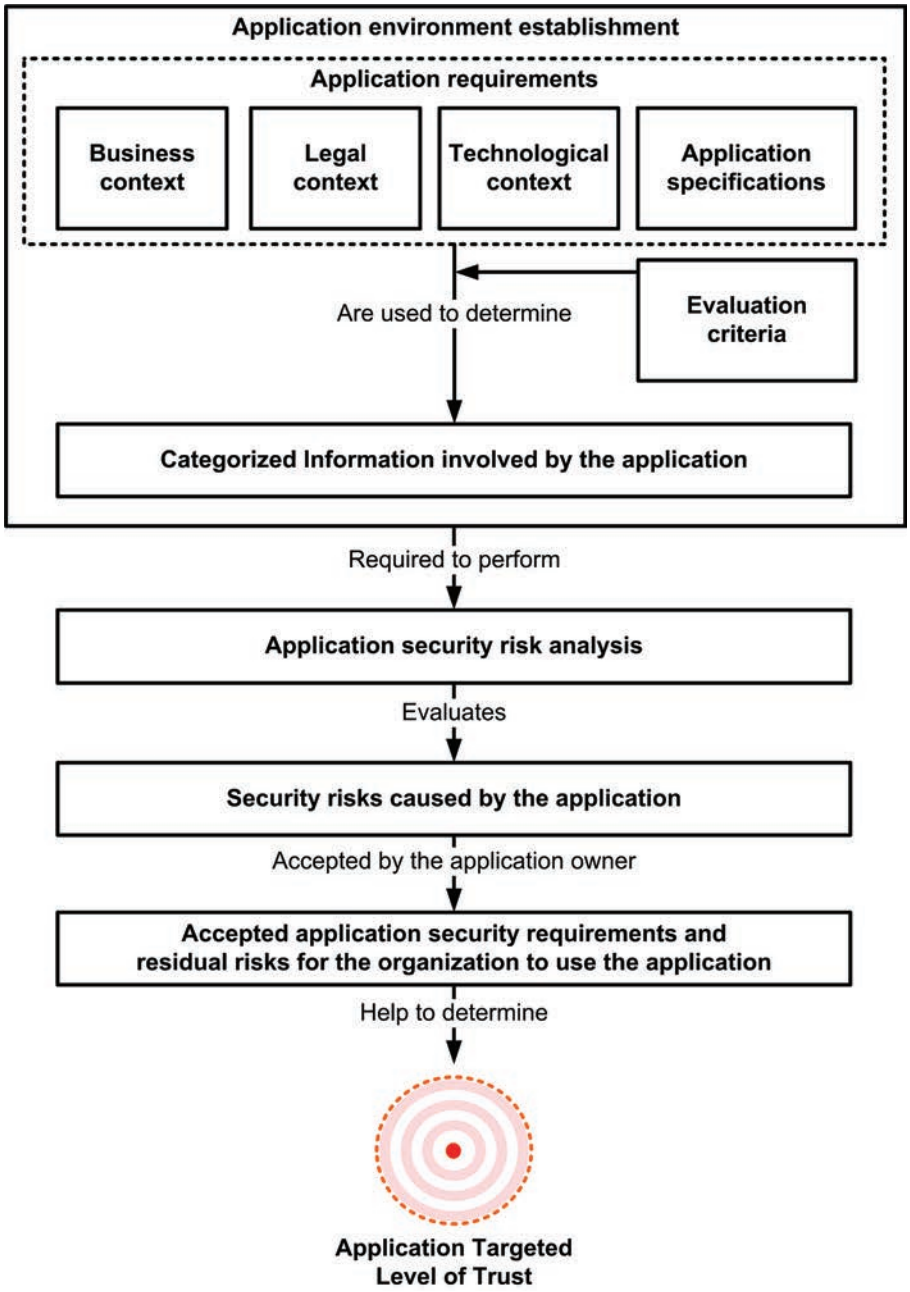

Figure 4 — Application security risk analysis as an essential step in determining the application's Targeted Level of Trust

Further guidance about the Application Security Risk Analysis Process will be provided in ISO/IEC 27034-3.

5.5.13 Application Security Verification Process

5.5.13.1 Purpose

The purpose of this process is to demonstrate an application's Actual Level of Trust at any time in the application's life cycle.

5.5.13.2 Description

This is a simple process by which a verification team checks the results of the verification measurements for each of the ASCs required by the application's Targeted Level of Trust.

5.5.13.3 Outcomes

As the result of performing this process:

a) the application's Actual Level of Trust is determined; and

b) if the application's Actual Level of Trust is equal to its Targeted Level of Trust, the application owner has documented evidence that the information security risk for this application has been reduced to an acceptable level.

5.5.13.4 Realization activities

Table 17 — RACI chart for realization of the application security verification process

Realization activities	Application owner	ONF Committee	Verification team	Domain expert	Auditor
1) For each ASC required by the application's Targeted Level of Trust, obtain the result of the verification measurement performed by an auditor, and verify that the result is positive	A	I	R	C	C

5.5.13.5 Guidance

A formal verification process, guided by verification policies, may be performed at any time during the application's life cycle and should be performed by an independent verification team with no involvement in application development projects.

Results of verification measurements for each ASC required by the application's Targeted Level of Trust should be obtained as required inputs.

ASCs provide verification measurements by diverse testing approaches, such as inspection, revision and unit testing. Other verification approaches can be used in later moments of the life cycle either as white box or black box testing, including integration testing or penetration testing.

An overview of this process is presented in ISO/IEC 27034-1:2011, Figure 14. A detailed description of the Application Security Verification Process is the subject of ISO/IEC 27034-4 and further guidance will be provided in that International Standard.

Annex A
(informative)

Aligning the ONF and ASMP with ISO/IEC 15288 and ISO/IEC 12207 through ISO/IEC 15026-4

A.1 General

ISO/IEC 15026-4 (Systems and software engineering — Systems and software assurance — Part 4:Assurance in the life cycle) gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties.

ISO/IEC 15026-4 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. If the stakeholders determine the specific property selected for special attention and justification through an assurance claim is application security, the ASMP provides a framework for achieving the claim.

A.2 Mapping

The table below provides a mapping of the ISO/IEC 15026-4 subclauses, ISO/IEC 15288 and ISO/IEC 12207 subclauses, ASMP element, and role of the ASMP element in the ISO/IEC 15026 (all parts) critical processes for achieving a claim of application security.

NOTE 1 While all processes in ISO/IEC 15288 and ISO/IEC 12207 contribute to the development efforts, it is the processes deemed critical in ISO/IEC 15026 (all parts) that are most relevant to the ONF and ONF management processes. Similar to the conformance criteria in ISO/IEC 15026 (all parts), the Agreement, Project, Technical, and Software Specific processes of ISO/IEC 12207:2008 are expected but not the focus of this mapping.

NOTE 2 ISO/IEC 27034-3 contains the application security processes and additional relationships and alignment to the management and technical processes in ISO/IEC 15288 and ISO/IEC 12207.

NOTE 3 ISO/IEC 27034-4 contains application security validation processes that measure the application's actual level of trust.

Table A.1 — Mapping of ISO/IEC 15026-4, ISO/IEC 15288, ISO/IEC 12207 and ISO/IEC 27034 subclauses

ISO/ IEC 15026-4 subclause	ISO/IEC 15288 and ISO/IEC 12207 subclause	Process element (per ISO/ IEC 27034-1)	Role of the ASMP element in the ISO/ IEC 15026 (all parts) critical processes
7.2 Acquisition process	ISO/IEC 15288:2008, 6.1.1 ISO/IEC 12207:2008, 6.1.1	7.3.5 Provisioning and operating the application	If the ASMP is established for an application or software that will be acquired, the project should ensure that the agreement considers the acquirer's application security practices/ expectations throughout the life cycle for the application element being acquired. Considerations for the provisioning and operation of the application should include conformance with the acquirer's security processes (or process expectations) for the application element being acquired, acceptance criteria, delivery mechanisms, the possibility of compromise during delivery, detection of anomalies, detection of counterfeits in the application element at arrival, expectations for defect resolution and patch management, etc.
7.3 Supply process	ISO/IEC 15288:2008, 6.1.2 ISO/IEC 12207:2008, 6.1.2	7.3.5 Provisioning and operating the application	If the ASMP is established for an application or software that will be supplied to an acquirer, the ASMP should be established to ensure the supplier provides the acquirer with a product or service that meets agreed requirements. Considerations for the provisioning and operation of the application should include review of the supplier's security processes for the application element being acquired, acceptance criteria, delivery mechanisms, the possibility of compromise during delivery, detection of anomalies, detection of counterfeits in the application element at arrival, expectations for defect resolution and patch management, etc.
7.4 Project planning process	ISO/IEC 15288:2008, 6.3.1 ISO/IEC 12207:2008, 6.3.1	7.3.4 Creating and maintaining the Application Normative Framework	The Project planning processes should leverage the ASMP and subsequent ANF to define and maintain a life cycle model that comprises stages using the defined application security life cycle models of the organization. When implemented, the Life Cycle Model Management Process should leverage the ASMP to establish standard life cycle models for application security for the organization. The Project planning process should tailor these organizational processes to meet the specific project needs.
7.5 Decision Management process	ISO/IEC 15288:2008, 6.3.3 ISO/IEC 12207:2008, 6.3.3	7.3.5 Provisioning and operating the application	Decision Management Process activities need to ensure that the consequences and impacts of application security are considered whenever a decision is made during provisioning and operating the application.

Table A.1 *(continued)*

ISO/ IEC 15026-4 subclause	ISO/IEC 15288 and ISO/IEC 12207 subclause	Process element (per ISO/ IEC 27034-1)	Role of the ASMP element in the ISO/ IEC 15026 (all parts) critical processes
7.6 Risk Management process	ISO/IEC 15288:2008, 6.3.4 ISO/IEC 12207:2008, 6.3.4	7.3.5 Provisioning and operating the application	Application security related project risks should be thoroughly integrated throughout the risk management process in priority setting, decision making, establishing and maintaining the risk profile, and risk treatment. Provisioning and operating the application and related risks should be realistically considered, including the risks of having to redo parts of the application. The project should evaluate the potential for not being able to achieve the necessary application security, resulting in a risk to the system certification or accreditation or resulting in the software not being used as intended.
7.7 Configuration management process	ISO/IEC 15288:2008, 6.3.5 ISO/IEC 12207:2008, 6.3.5	7.3.5 Provisioning and operating the application	The Configuration Management Process establishes and maintains the integrity of all identified artefacts of a project or process and makes them available to concerned parties. Provisioning and operating the application has two relationships relevant to application security: (1) effective configuration management of the application elements to ensure application security and (2) the information showing achievement of application security itself is under configuration management. NOTE Additional guidance for these configuration management practices is available in ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls, and ISO 10007:2003, Quality management systems – Guidelines for configuration management.
7.8 Information Management process	ISO/IEC 15288:2008, 6.3.6 ISO/IEC 12207:2008, 6.3.6	7.3.5 Provisioning and operating the application	For application security, the Information Management process provides the information about the achievement of application security to the relevant stakeholders and provides for delivery of the body of information showing achievement of application security to relevant stakeholders, including regulatory or approval authorities.
7.9 Stakeholder Requirements Definition process	ISO/IEC 15288:2008, 6.4.1 ISO/IEC 12207:2008, 6.4.1	7.3.2 Specifying the application requirements and environment	The Stakeholder Requirements Definition Process defines the requirements for a system that can provide the services needed by users and other stakeholders in a defined environment. It analyzes and transforms these into a common set of stakeholder requirements. As a subset of these requirements, the Targeted Level of Trust and application security properties for which a high degree of confidence is required for their achievement are identified and documented.

Table A.1 *(continued)*

ISO/ IEC 15026-4 subclause	ISO/IEC 15288 and ISO/IEC 12207 subclause	Process element (per ISO/ IEC 27034-1)	Role of the ASMP element in the ISO/ IEC 15026 (all parts) critical processes
7.10 Requirements Analysis process	ISO/IEC 15288:2008, 6.4.2 ISO/IEC 12207:2008, 6.4.2	7.3.3 Assessing application security risks	The Requirements Analysis Process transforms the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services at the Targeted of Level of Trust. Requirements analysis should include an assessment of application security risks and adequacy of associated application security requirements related but not limited to the functional boundary of the system, functions that the system is required to perform, necessary implementation constraints that are introduced by stakeholder requirements or are unavoidable solution limitations, measures that enable the assessment of technical achievement.
7.11 Verification process	ISO/IEC 15288:2008, 6.4.6	7.3.6 Auditing the security of the application	In the context of the ASMP, the Verification Process confirms that the specified Targeted Level of Trust is achieved. The results should include the information required to effect the remedial actions that correct non-conformances in the realized application or the processes that act on it and account for uncertainty in verification activities such as test tool reliability and level of the uncertainty in results (i.e. rates of false positives and false negatives). The ASMP should consider validation evidence created throughout the life cycle. For example, testing for code weaknesses in the development process or during sustainment.
7.12 Operation process	ISO/IEC 15288:2008, 6.4.9 ISO/IEC 12207:2008, 6.4.9	7.3.5 Provisioning and operating the application	The Operation Process involves provisioning and operating the application in order to deliver its services in its intended environment and provides support to the customers of the software product. Plans for this process should consider achievement of application security throughout the life of the system, operational restrictions, and consistency of assumptions from the approach to application security. The project should establish reporting systems and procedures for investigation and disposition of application security related incidents.
7.13 Maintenance process	ISO/IEC 15288:2008, 6.4.10 ISO/IEC 12207:2008, 6.4.10	7.3.5 Provisioning and operating the application	Plans for maintenance during provisioning and operating the application should consider application security throughout the life of the system. The project should ensure that the maintenance plan provides for evaluating the effect on application security from changes made to the application or system elements during maintenance and maintaining appropriate evidence that the Targeted Level of Trust is achieved.

Annex B
(informative)

ONF implementation example: implementing ISO/IEC 27034 Application Security and its ONF in an existing organization

B.1 General

In this example, a financial institution starts a project to implement the ISO/IEC 27034 Application Security International Standard and its ONF in order to improve the security of its applications and to harmonize management of security controls throughout its application development projects.

The organization has decided to implement ISO/IEC 27034 using a step by step approach, by realizing the project in progressive phases, each with its own scope. This example shows only the first phase of the project.

The organization divides the project into six sub projects as schematized in Figure B.1:

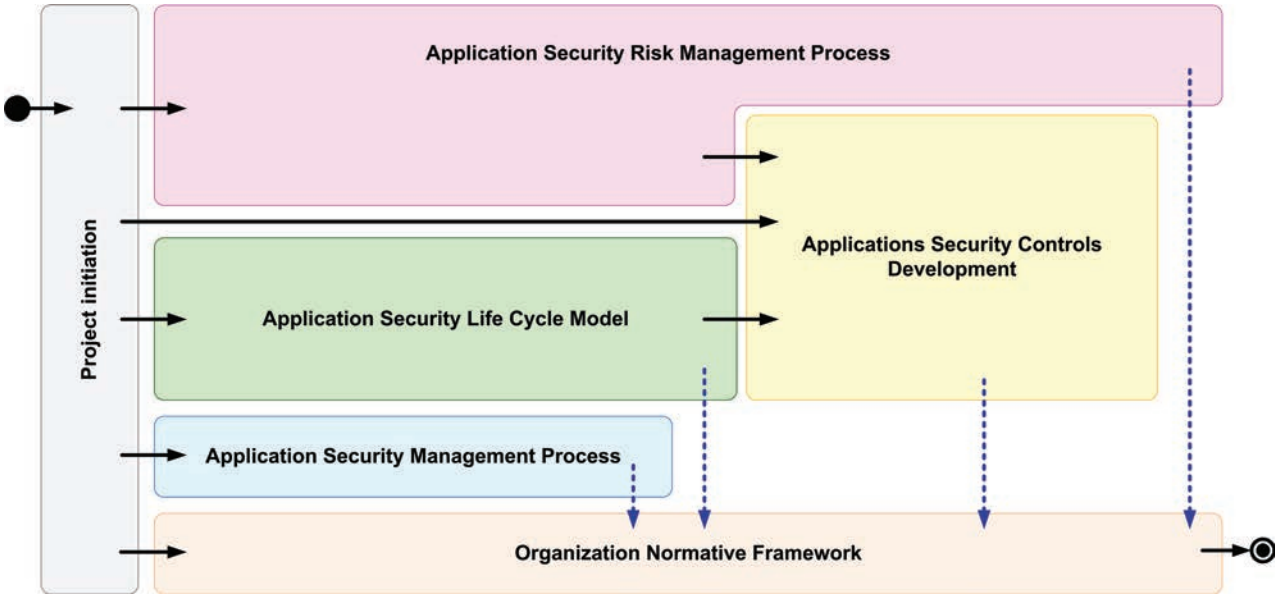

Figure B.1 — Implementing the ONF in an organization – sub projects overview

B.1.1 Project Initiation

B.1.1.1 Purpose

The purpose of this sub project is to:

a) define an acceptable and manageable scope for the project and for each sub project;

b) assign project teams;

c) determine the structure of ASCs to be developed; and

d) monitor the sub projects.

B.1.1.2 Sub project overview

Figure B.2 below shows a graphical representation of this sub project.

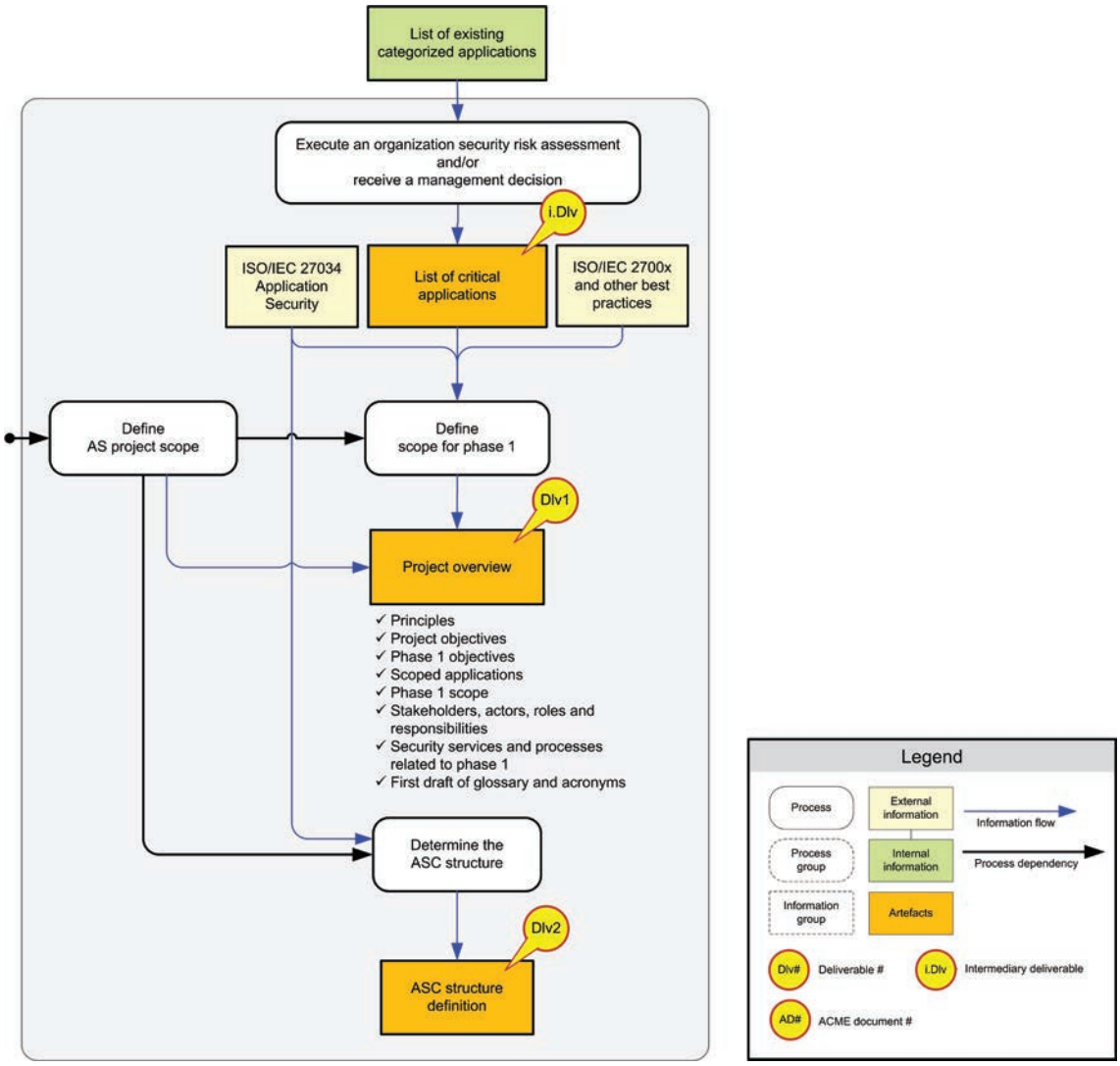

Figure B.2 — Application Security ONF Implementation Project, phase 1

B.1.1.3 Actors

Actors involved in this sub project are:

a) top management; and

b) project manager.

B.1.1.4 Inputs

The input for this sub project is a list of existing categorized applications (as provided by the information security management system).

B.1.1.5 Activities

As shown on Figure B.2 above, activities for this sub project are:

a) define application security project scope;

b) execute an organization security risk assessment and/or receive a top management decision;

c) define scope for phase 1 of the project according to item b) above; and

d) determine the ASC structure.

B.1.1.6 Outcomes

Outcomes of this sub project are the following deliverables:

a) iDiv. – list of critical applications;

b) Dlv 1 – project overview providing the following information:

   1) principles;

   2) project objectives;

   3) phase 1 objectives;

   4) scoped applications;

   5) phase 1 scope;

   6) stakeholders, actors, roles, responsibilities;

   7) security services and processes related to phase 1;

   8) first draft of glossary and acronyms;

c) Dlv 2 – ASC structure definition.

B.1.2 Application Security Risk Management sub-project

B.1.2.1 Purpose

During this sub project, the organization will plan, perform, maintain and support the:

a) development of an application security risk management process adapted to the organization's actors, contexts and application specifications,

b) identification of security risks from the organization's use of its critical applications, and

c) identification of security requirements that must be addressed by ASCs.

B.1.2.2 Actors

Actors involved in this sub project are the IT security risk management group.

B.1.2.3 Sub project overview

Figure B.3 below shows a graphical representation of this sub project.

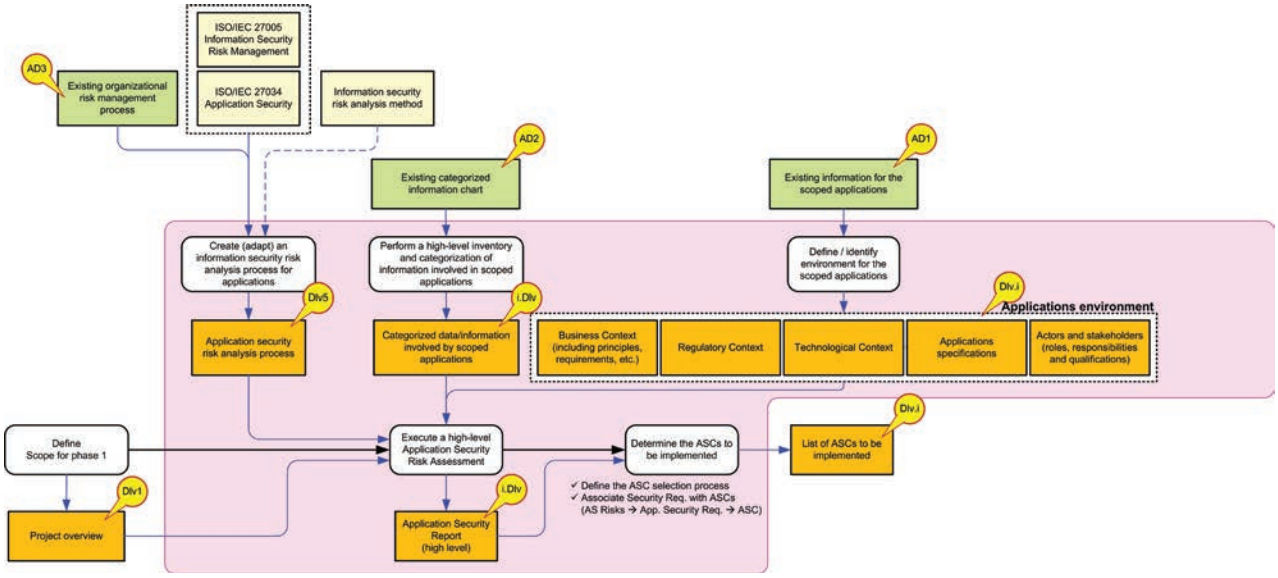

Figure B.3 — Application Security Risk Management Process sub project

B.1.2.4 Inputs

Inputs for this sub project are:

a) information security risk analysis method;

b) AD 1 – existing information for the scoped applications;

c) AD 2 – existing categorized information chart;

d) AD 3 – existing organizational risk management process; and

e) Dlv 1 – project overview.

B.1.2.5 Activities

Activities for this sub project are:

a) create (adapt) an information security risk process for applications;

b) realize a high-level inventory and categorization of information involved in scoped applications;

c) define / identify environment for the scoped applications;

d) execute a high-level application security risk assessment;

e) determine the ASCs to be implemented:

   1) define the ASC selection process;

   2) associate security requirements with ASCs (security risks → security requirements → ASCs).

B.1.2.6 Outcomes

Outcomes of this sub project are:

a) Dvl 5 – application security risk analysis process;

b) i.Dvl – categorized data/information involved by the scoped applications;

c) i.Dlv – applications environment:

   1) business context (including principles, requirements, etc.);

   2) regulatory context;

   3) technological context;

   4) applications specifications;

   5) actors and stakeholders (roles, responsibilities and qualifications);

d) i.Dlv – application security report (high level);

e) i.Dlv – list of ASCs to be implemented.

B.1.3 Application Life Cycle Model sub-project

B.1.3.1 Purpose

During this sub project, the organization will plan, perform, maintain and support the:

a) harmonization of methods, processes and activities present in different life cycles in the organization,

b) collaboration of appropriate accountable management and groups involved in governance, architecture, compliance, development, operation, IT, verification and audit, and

c) determination of life cycle stages in scope of phase 1.

B.1.3.2 Actors

Actors for this sub project are:

a) compliance practices group;

b) IT application development practices group;

c) governance and project management practices group;

d) security integration in projects group; and

e) security architecture practices group.

B.1.3.3 Sub project overview

Figure B.4 below shows a graphical representation of this sub project.

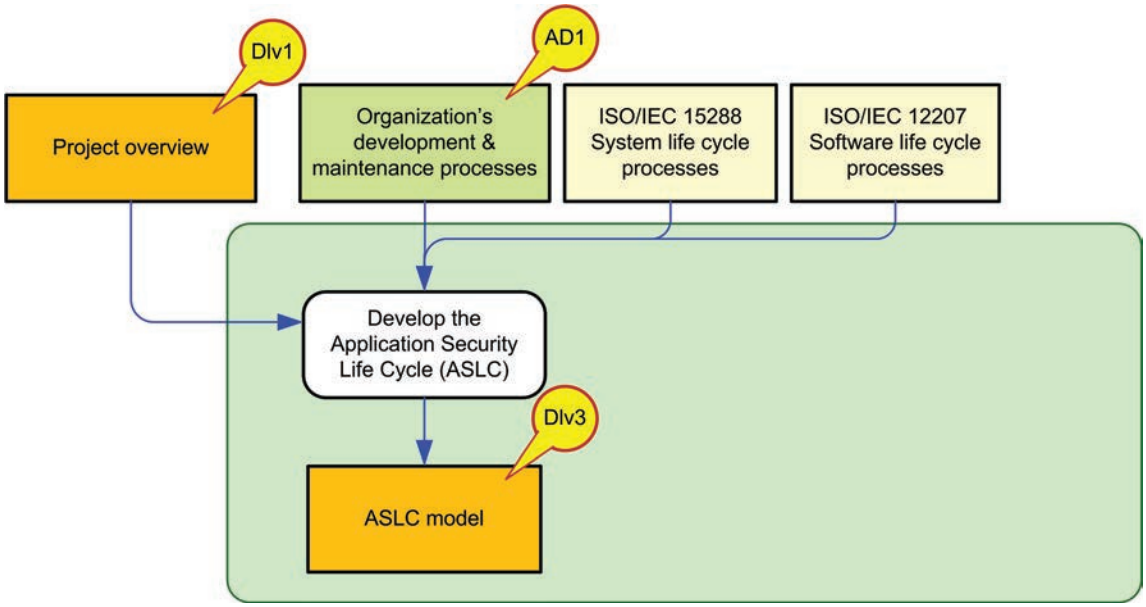

Figure B.4 — Application Security Life Cycle Model sub project

B.1.3.4 Inputs

The inputs for this sub project are:

a) AD 1 – Organization's development and maintenance processes; and

b) Dlv 1 – Project overview.

B.1.3.5 Activities

The activity for this sub project is: Develop the application security life cycle (ASLC) for the organization.

B.1.3.6 Outcomes

The outcome of this sub project is: Dlv 3 – ASLC model

B.1.4 Application security management process sub project

B.1.4.1 Purpose

During this sub project, the organization will plan, perform and maintain the development and maintenance of an application security management process adapted to the organization and compliant with the requirements in ISO/IEC 27034.

B.1.4.2 Actors

Actors for this sub project are:

a) software development practices group;

b) governance and project management practices group; and

c) security integration in projects group.

B.1.4.3 Sub project overview

Figure B.5 below shows a graphical representation of this sub project.

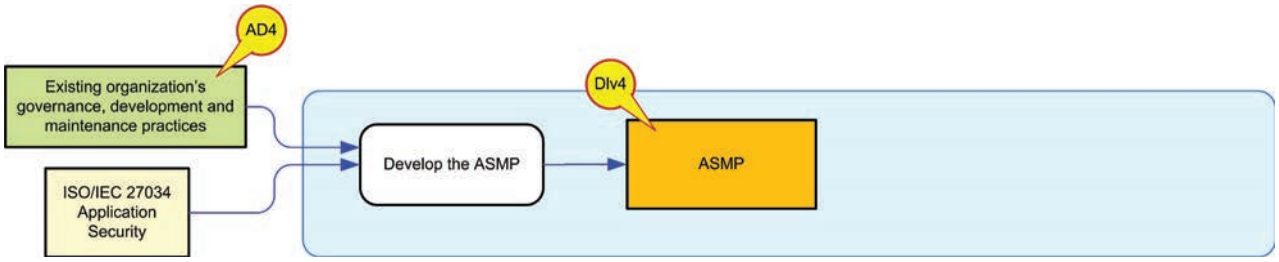

Figure B.5 — Application Security Management Process sub-project

B.1.4.4 Inputs

The input for this sub project is: AD 4 – Existing organization's governance, development and maintenance practices.

B.1.4.5 Activities

The activity for this sub project is: Develop the organization's application security management process.

B.1.4.6 Outcomes

The outcome of this sub project is: Dlv 4 – ASMP (documentation and guidance for integrating application security in a project)

B.1.5 Organization Normative Framework sub-project

B.1.5.1 Purpose

During this sub project, the organization will plan, perform, maintain and support the:

a) nomination of ONF committee members,

b) development of ONF management and maintenance processes, and

c) consolidation of application security elements in an authoritative repository, available to all concerned.

B.1.5.2 Actors

Actors for this sub project are:

a) compliance practices group;

b) IT applications development practices group;

c) governance and project management practices group;

d) operations and IT infrastructure practices group; and

e) governance – project management support group.

B.1.5.3 Sub project overview

Figure B.6 below shows a graphical representation of this sub project.

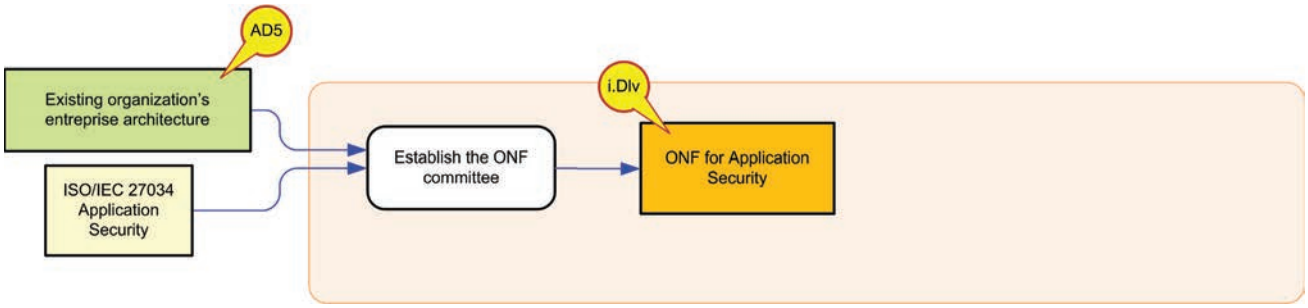

Figure B.6 — Organization Normative Framework sub project

B.1.5.4 Inputs

The input for this sub project is: Existing organization's enterprise architecture.

B.1.5.5 Activities

The activity for this sub project is: start the ONF committee.

B.1.5.6 Outcomes

The activity for this sub project is: i.Dlv - Organization normative framework for application security.

B.1.6 Applications Security Controls Development sub-project

B.1.6.1 Purpose

During this sub project, the organization will plan, perform, maintain, support and audit the:

a) development of ASCs according to the organization's application security requirements,

b) validation, verification, testing, implementation and audit of developed ASCs,

c) alignment of ASCs to the application security life cycle model,

d) management of an ASC development and maintenance process,

e) development of training for people who will develop and validate ASCs, and

f) development of training for people who will implement, verify and audit ASCs.

B.1.6.2 Actors

Actors for this sub project are:

a) owners of scoped applications;

b) compliance practices group – information security controls framework team;

c) software development practices group; and

d) IT applications development practices group.

B.1.6.3 Sub project overview

Figure B.7 below shows a graphical representation of this sub project.

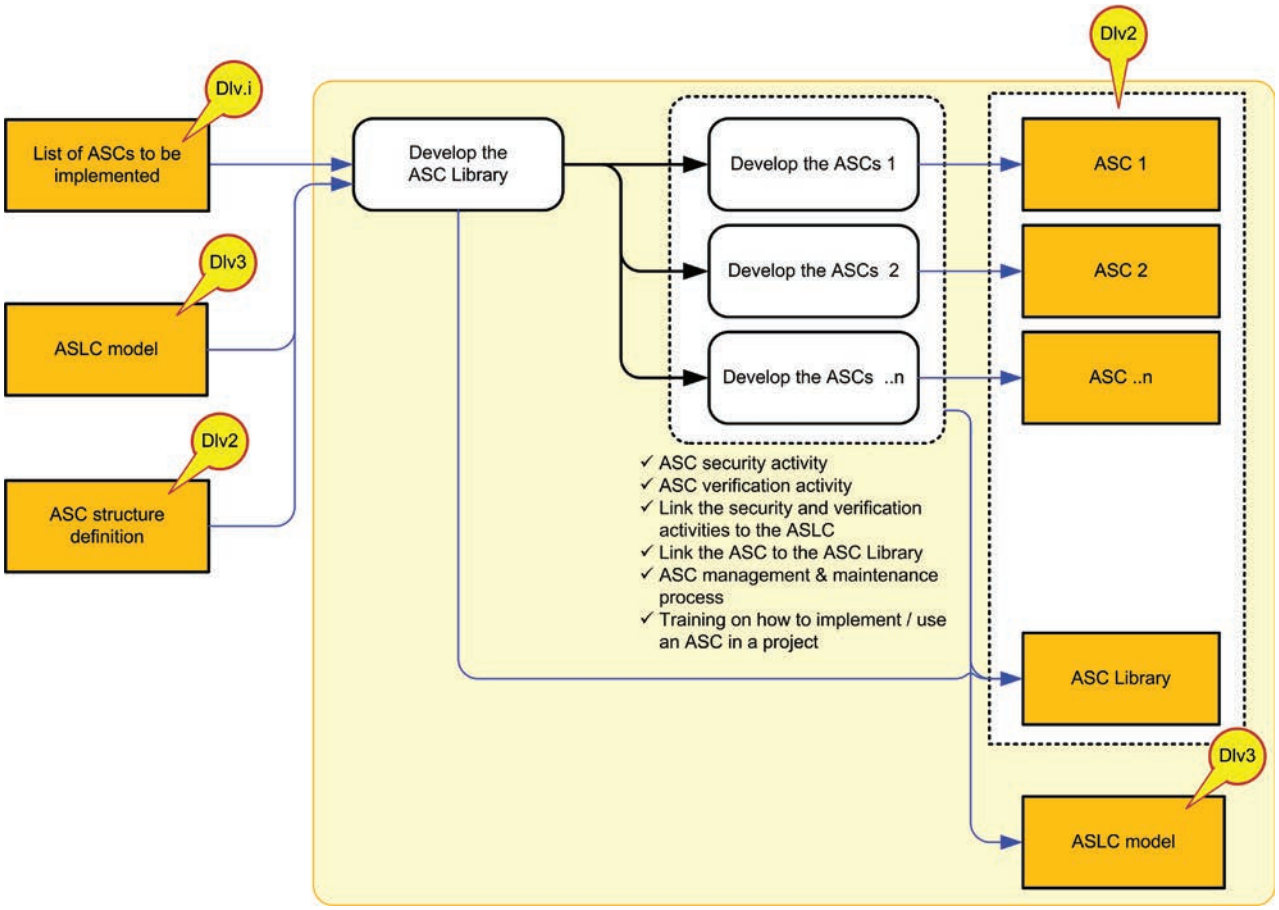

Figure B.7 — Applications Security Controls Development sub project

B.1.6.4 Inputs

Inputs for this sub project are:

a) i.Dlv – List of ASCs to be implemented;

b) Dlv 2 – ASC structure definition; and

c) Dlv 3 – ASLC Model.

B.1.6.5 Activities

Activities for this sub project are:

a) develop the ASC Library;

b) develop the ASCs 1, 2 to 'n':

1) develop the ASC security activity;

2) develop the ASC verification activity;

3) link the security and verification activities to the ASLC model;

4) link the ASC to the ASC Library;

5) develop the ASC management and maintenance process;

6) develop guidance or training on how to implement / use this ASC in a project.

B.1.6.6 Outcomes

Outcomes of this sub project are:

a) ASCs;

b) ASC Library; and

c) Dlv 3 – ASLC Model (updated).

B.2 Complete project workflow diagram

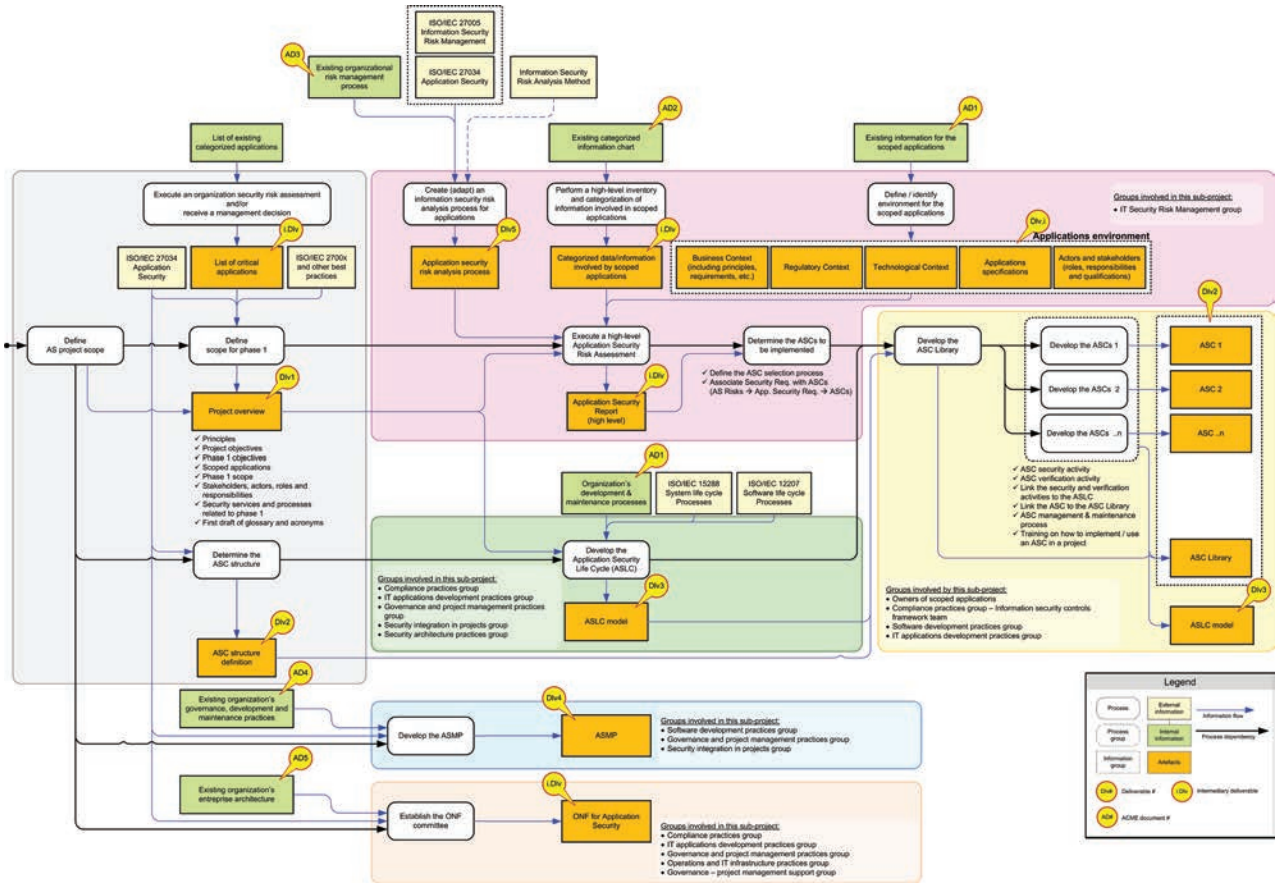

Figure B.8 — ONF Implementation example: implementing ISO/IEC 27034 Application Security and its ONF in an organization — Overview diagram

Bibliography

[1] ISO/IEC 33001:2015, *Information technology — Process assessment – Part 1: Concepts and terminology*

[2] ISO/DIS 19011:2011, *Information technology — Security techniques — Guidelines for auditing management systems*

[3] ISO/IEC/TR 20000-4:2010, *Information technology — Service management — Part 4: Process reference model*

[4] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[6] ISO/IEC 27036-1:2014, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

ICS 35.040

Price based on 52 pages